Abstract

This document presents and discusses different use-case scenarios of mobility anchor selection in Distributed Mobility Management (DMM).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 12, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must...
Table of Contents

1. Terminology .................................................. 3
2. Introduction .................................................. 4
3. Considered contexts .......................................... 5
   3.1. Mobile node context ...................................... 5
   3.2. Application context ...................................... 6
   3.3. Network context .......................................... 8
4. Use-case scenarios ............................................. 9
   4.1. Extremely mobile nodes without any typical location ... 9
   4.2. Mobile nodes with one or more typical locations ...... 10
   4.3. Fairly stationary nodes ................................ 12
5. Security Considerations ........................................ 13
6. IANA Considerations ........................................... 14
7. Acknowledgements ............................................. 15
8. References ..................................................... 16
   8.1. Normative References .................................... 16
   8.2. Informative References .................................. 16
Authors’ Addresses ............................................... 17
1. Terminology

IP-handover:
   a handover of a mobile node at the IP level resulting in an IP address change at the mobile node.

New flow:
   a flow that did not undergo any IP-handover.

Handover flow:
   a flow that did undergo one or more IP-handovers.

New traffic:
   the data traffic of the new flows.

Handover traffic:
   the data traffic of the handover flows.

Current access router:
   the access router where the mobile node is currently attached at the IP level.

DMM default mode of mobility anchor selection:
   new flows are always anchored at the current access router which acts as the mobility anchor for these flows after an IP-handover.
2. Introduction

Distributed Mobility Management (DMM) aims at overcoming the shortcomings of the existing IP mobility protocols, such as Mobile IPv6 [RFC6275] and Proxy Mobile IPv6 [RFC5213], that are considered centralized. It brings the mobility anchor closer to the mobile node, down at the access routers level. This is the enabler of a concept that is so-called dynamic mobility, where the mobile node changes its mobility anchor for new flows. New flows are always initiated using the mobile node’s current IP address which is configured using the prefix provided by the current access router. The data traffic of these flows is then routed optimally until the mobile node undergoes an IP-handover. However, upon an IP-handover, tunneling mechanisms are needed with that access router, which is then considered the mobility anchor of those flows initiated using its prefix during the whole lifetime of those flows. In what follows, this is considered the DMM default mode of mobility anchor selection.

If most of the flows are short enough to not undergo one or more IP-handovers, it is expected that most of the data traffic is routed optimally. However, this assumption is not always valid and the mobility anchor for new flows, when initiated, could be selected in a more appropriate manner.

When a flow is initiated, it is assigned a mobility anchor that lasts during its whole lifetime. Thus, selecting the most appropriate mobility anchor for a flow when initiated can significantly enhance the mobility management performance, e.g. less overhead, shorter end-to-end delay. Thus, a DMM solution should allow selecting and using the most appropriate mobility anchor among a set of distributed ones [I-D.ietf-dmm-best-practices-gap-analysis]. In order to achieve this, different metrics and contexts should be taken into consideration. Distributing the mobility anchor functionalities at the access routers level allows considering several contexts such as the mobile node’s mobility context, the application context, and the network context.

Hereafter in this document, the considered contexts are presented and then the different use-case scenarios are discussed.
3. Considered contexts

3.1. Mobile node context

The mobile node’s mobility has an important effect on the mobility anchor selection. For example, a mobile node with high mobility undergoes frequent IP-handovers. When considering DMM default mode of mobility anchor selection, almost all the traffic of such mobile node is handover traffic, moreover, the number of simultaneous anchors and tunnels may increase. On the other hand, flows of mobile nodes with low mobility are more likely to be initiated and terminated before undergoing an IP-handover.

In addition, the mobile node’s location with respect to the different mobility anchors influences selecting one of them for new flows. For example, locating the mobility anchor as close as possible to the mobile node results in a shorter tunnel, and hence less tunneling overhead, when tunneling mechanisms are required. The most appropriate mobility anchor is the closest one to the mobile node during the longer portion of the flow lifetime. At the instant of initiating a new flow, the current access router is the closest one to the mobile node. However, the mobile node may undergo an IP-handover and attach to another access router. Whether the longer portion of the flow is before or after the IP-handover has an effect on selecting the most appropriate mobility anchor for this flow.

Moreover, a mobile node may have one or more "typical locations" where it attaches to the network most of the time, e.g. at home. This helps expecting the mobile node’s location for relatively long durations and, consequently, in selecting the most appropriate mobility anchor by using information about typical location(s). Note that some statistics show that users spend more than 60% of their time at home and work [Cisco-VNI].

Finally, the mobile node’s attachments history is needed in order to take into consideration the mobile node’s mobility and location as described above.
3.2. Application context

Based on the application, the need of IP continuity and the flow characteristics can be estimated. While applications that require IP continuity cause the establishment of tunnels in the access network upon an IP-handover, applications that can tolerate an IP address change at the application layer, e.g. SIP-based sessions, do not [I-D.ietf-dmm-requirements]. The mobility anchor selection is less important in the latter case due to the capability of changing the IP address. In fact, there is no need for tunneling and hence no need for a mobility anchor since the application can tolerate any change in the IP address; hence, all the traffic is routed using standard routing schemes.

In addition, the flow characteristics are highly dependent on the application. Some applications generate in general long flows such as multimedia (e.g. video streaming), online gaming, large files downloading, etc. (see Table 1 below); others generate in general short flows such as TCP connections for HTTP and SMTP sessions. Long flows are more likely to undergo one or more IP-handovers and therefore the mobility anchor selection can play an important role to enhance the mobility management performance. On the other hand, short flows are more likely to be initiated and terminated before an IP-handover.

In the following table, we present some examples on different types of applications. For each application, we mention the expected (or probable) traffic and mobility characteristics as well as the possible types of devices used for such application. The objective of this list of applications is to show later some possible real mapping(s) for the different use-case scenarios.
<table>
<thead>
<tr>
<th>Application</th>
<th>Traffic Type</th>
<th>Mobility Nature</th>
<th>User Device</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>RT Gaming</td>
<td>Long flows</td>
<td>Stationary</td>
<td>Laptop, tablet, smartphone, game</td>
<td>For game consoles, the device and traffic characteristics could be easily predicted</td>
</tr>
<tr>
<td></td>
<td>with IP req</td>
<td>or mobile (depending on game)</td>
<td>console</td>
<td></td>
</tr>
<tr>
<td>Audio/Video</td>
<td>Long flows</td>
<td>Stationary</td>
<td>Smartphone, tablet, laptop</td>
<td></td>
</tr>
<tr>
<td>conferencing</td>
<td>with IP req</td>
<td>or mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Live</td>
<td>Long flows</td>
<td>Stationary</td>
<td>Large screen TV, laptop, tablet,</td>
<td>If a large screen TV, client is stationary. Otherwise, client is mobile</td>
</tr>
<tr>
<td>streaming</td>
<td>with IP req</td>
<td>or mobile</td>
<td>smartphone</td>
<td></td>
</tr>
<tr>
<td>IPTV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Waze</td>
<td>Long flows</td>
<td>Mobile</td>
<td>Smartphone, dedicated car GPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>without IP req</td>
<td></td>
<td>(future)</td>
<td></td>
</tr>
<tr>
<td>GoPro</td>
<td>Long flows</td>
<td>Mobile</td>
<td>GoPro camera</td>
<td>A typical location (Ski resort)</td>
</tr>
<tr>
<td></td>
<td>with IP req</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Report</td>
<td>Long flows</td>
<td>Stationary</td>
<td>Mobile surveillance, HD camera</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with IP req</td>
<td>or mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Video streaming in vehicles</strong></td>
<td><strong>Long flows with IP continuity req</strong></td>
<td><strong>Mobile</strong></td>
<td><strong>Car TV, tablet, smartphone</strong></td>
<td><strong>If the car is mainly used in specific neighborhood da typical location i srelevant</strong></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------</td>
<td>------------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Camcorder download</strong></td>
<td><strong>Long flows with IP continuity req</strong></td>
<td><strong>Stationary or mobile</strong></td>
<td><strong>Camcoder</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HTTP and SMTP sessions</strong></td>
<td><strong>Short flows with IP continuity req</strong></td>
<td><strong>Stationary or mobile</strong></td>
<td><strong>Smartphone, tablet, laptop</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Table 1**

3.3. Network context

When a mobility anchor is assigned to a flow (when the flow is initiated), it acts as a mobility anchor for this flow the whole flow’s lifetime. It is responsible to forward the flow’s data packets if the mobile node is physically attached to it. It is responsible, in addition, to encapsulate and de-capaculate the flow’s data packets if the mobile node is not attached to it and tunneling mechanisms are used.

Even with distributed mobility anchors, the distribution of the active mobile nodes in the network is not necessarily even. As a result, some mobility anchors are overloaded more than others. It is then reasonable to take into consideration the estimated (or projected) level of load of the mobility anchors as well as the access network characteristics/resources when selecting one of them for a new flow (the metrics for measuring this level are left for specific implementations).
4. Use-case scenarios

4.1. Extremely mobile nodes without any typical location

Extreme mobility could be due to either a high mobile node’s speed, or a small access router’s coverage area, or both.

Scenario 1: running applications generating typically short flows

Short flows are more likely to be initiated and terminated before the mobile node undergoes an IP-handover. Even if a flow experiences an IP-handover, it is expected that the flow does not last long after the IP-handover. In other words, most of the mobile node’s traffic is new traffic in this scenario. As a result, the closest mobility anchor to the mobile node during the longest portion of a flow is its current access router. It is recommended then to always anchor new flows at the current access router, which is the DMM default mode of mobility anchor selection.

A well known example on short flows is the TCP connections for HTTP and SMTP sessions.

Scenario 2: running applications generating typically long flows

For extremely mobile nodes, it is more likely that a flow experiences an IP-handover soon after being initiated. And since the flows are long-lived, it is expected that a flow lasts for a long duration after the IP-handover(s). As a result, it could be said that most of the traffic is handover traffic in this scenario. Whatever is the mobility anchor selection criterion, most of (almost all) the mobile node’s data traffic needs tunneling mechanisms. Thus, the mobility anchor selection cannot play a significant role regarding the route optimization or the tunneling overhead reduction.

However, there are number of consequences regarding the control plane e.g. number of simultaneous anchors/tunnels for a mobile node and the related contexts and signaling loads. First, let us consider the DMM default mode of mobility anchor selection. Since new flows are always anchored at the current access router, each flow initiated between two consecutive IP-handovers is anchored at a different mobility anchor. With extremely mobile node, long flows are expected to experience several IP-handovers and their mobility anchors are expected to be maintained for a long duration. As a result, the number of simultaneous anchors/tunnels for a mobile node may increase as well as the related contexts and signaling loads.
signaling loads. This affects the control plane negatively.

As the DMM default mode does not achieve data plane optimization in the scenario described above, it is reasonable to consider a more centralized approach for mobility anchor selection in order to reduce the negative effects on the control plane. If data packets are going to be tunneled in both cases, managing a single tunnel to a single mobility anchor would be better than managing several tunnels to several mobility anchors at the same time.

It is worth mentioning that the discussion above is considering applications that require IP-address continuity. On the other hand, there is no issue regarding the applications that allow an IP address change and manage mobility at the application layer since they do not need mobility anchors as mentioned before.

Some examples on this scenario are (cf. Table 1) RT gaming, audio/video conferencing, live streaming IPTV, video report, video streaming in vehicles, and camcorder download.

Scenario 3: running applications generating both long and short flows

In this case, short and long flows can be distinguished when selecting a mobility anchor for a flow, based on scenario 1 and scenario 2. Short flows are always anchored at the current access router; long flows are anchored based on a more centralized approach. In this way, data packets of short flows are generally routed optimally and long flows do not introduce a large number of simultaneous anchors/tunnels.

4.2. Mobile nodes with one or more typical locations

Scenario 4: running applications generating typically short flows

As the flows are short, there is no expected benefit from having a typical location. If initiated when the mobile node is not at its typical location, such flows are more likely to end quickly before the mobile node goes back to its typical location. Otherwise, they would be initiated and terminated when the mobile node is at its typical location. As a result, the current access router is always the best mobility anchor for new flows and hence the DMM default mode of mobility anchor selection fits well this scenario.

When the car is used mainly for short distance usages, Waze (cf. Table 1) could be an example on this scenario.
Scenario 5: running applications generating typically long flows

In this scenario, having a typical location is expected to be beneficial for the mobile node’s mobility anchor selection. As mentioned before, the best mobility anchor for a flow is the closest one to the mobile node during the longer portion of this flow. Then, the best mobility anchor for a flow could be in some cases that of the typical location even if the flow is not initiated there. For example, if the mobile node initiates a long flow and then comes back (undergoing an IP-handover) quickly to its typical location, the longer portion of the flow would be after the IP-handover. Thus, it is reasonable to select the typical location’s mobility anchor for such flow when initiated. This results in tunneling part of the flow’s data traffic when initiated but in routing optimally most of it afterwards.

The analysis described above would be still valid if the mobile node has more than one typical location. However, the benefits may not be in some cases as great as those of the one typical location scenario, depending on the mobile node’s movements. If there is no clear benefit from selecting one out of the mobility anchors, the network context (i.e. level of load on each mobility anchor) comes into play leaning towards selecting the mobility anchor that is less loaded. Another refinement is to add the time of day to the statistics collection in the mobile node’s attachments history. If it is noticed that one of the typical locations is more popular than the others, this helps in selecting a mobility anchor according to the time of attachment.

Some examples on this scenario are (cf. Table 1) RT gaming, audio/video conferencing, live streaming IPTV, GoPro, video report, video streaming in vehicles, and camcorder download.

Scenario 6: running applications generating both long and short flows

If it is possible, the short and long flows should be distinguished as follows. While short flows are assigned the closest mobility anchor which is the current access router, long flows are assigned the typical location’s mobility anchor. In this case, the mobile node uses several IP addresses simultaneously e.g. the one related to the typical location for all long flows and the current IP address for short flows. Hence, the mobile node needs a source address selection mechanism in order to distinguish between the different IP addresses when initiating a flow.
4.3. Fairly stationary nodes

Scenario 7: running similar or different applications

In fact, a fairly stationary node has one typical location for almost all the time. The mobile node selects always the typical location’s mobility anchor, which is the current access router most of the time.

Some examples on this scenario are (cf. Table 1) RT gaming, audio/video conferencing, live streaming IPTV, video report, and camcorder download.
5. Security Considerations

TBD.
6. IANA Considerations

This document has no actions for IANA.
7. Acknowledgements

The authors would like to express their gratitude to Wu-Chi Feng and Philippe Bertin for having discussions, sharing thoughts, or providing reviews on anchor selection in DMM.
8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Hassan Ali-Ahmad (Editor)
Orange
Email: hassan.aliahmad@orange.com

Danny Moses
Intel Corporation
Email: danny.moses@intel.com

Hassnaa Moustafa
Intel Corporation
Email: hassnaa.moustafa@intel.com

Pierrick Seite
Orange
Email: pierrick.seite@orange.com

Tiago Condexia
University of Aveiro
Email: tscondeixa@ua.pt
An IPv6 Distributed Client Mobility Management approach using existing mechanisms  
draft-bernardos-dmm-cmip-00

Abstract

The use of centralized mobility management approaches -- such as Mobile IPv6 -- poses some difficulties to operators of current and future networks, due to the expected large number of mobile users and their exigent demands. All this has triggered the need for distributed mobility management alternatives, that alleviate operators’ concerns allowing for cheaper and more efficient network deployments.

This draft describes a possible way of achieving a distributed mobility behavior with Client Mobile IP, based on Mobile IPv6 and the use of Cryptographic Generated Addresses.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 14, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction

Most of the currently standardized IP mobility solutions, like Mobile IPv6 [RFC6275], or Proxy Mobile IPv6 [RFC5213] rely to a certain extent on a centralized mobility anchor entity. This centralized network node is in charge of both the control of the network entities involved in the mobility management (i.e., it is a central point for the control signalling), and the user data forwarding (i.e., it is also a central point for the user plane). This makes centralized mobility solutions prone to several problems and limitations, as identified in [I-D.ietf-dmm-requirements]: longer (sub-optimal) routing paths, scalability problems, signaling overhead (and most likely a longer associated handover latency), more complex network deployment, higher vulnerability due to the existence of a potential single point of failure, and lack of granularity on the mobility management service (i.e., mobility is offered on a per-node basis, not being possible to define finer granularity policies, as for example per-application).

There are basically two main approaches that are being researched now: one aimed at making Mobile IPv6 work in a distributed way, and another one doing the same exercise for Proxy Mobile IPv6 (see the document [I-D.ietf-dmm-best-practices-gap-analysis]). In this draft we describe a solution to achieve a DMM behavior with a CMIP (MIPv6) solution. This document is based on a research paper of the same authors, called "Flat Access and Mobility Architecture: an IPv6 Distributed Client Mobility Management solution" [GOB+11].

2. Terminology

The following terms used in this document are defined in the Mobile IPv6 specification [RFC6275]:

- Home Agent (HA)
- Home Link
- Home Address (HoA)
- Care-of Address (CoA)
- Binding Update (BU)
- Binding Acknowledgement (BA)

The following terms are defined and used in this document:
DAR (Distributed Anchor Router). First hop routers where the mobile nodes attach to. They also play the role of mobility managers for the IPv6 addresses they anchor.

HDAR (Home Distributed Anchor Router). DAR which plays the role of Home Agent for a particular IPv6 address (i.e., DAR where that IPv6 address is anchored).

3. Description of the solution

Distributed Mobility Management approaches try to overcome the limitations of the traditional centralized mobility management, i.e., Mobile IP, by bringing the mobility anchor closer to the MN. Following this idea, in our approach -- that we call Flat Access and Mobility Architecture (FAMA) -- the MIPv6 centralized home agent is moved to the edge of the network, being deployed in the default gateway of the mobile node. That is, the first elements that provide IP connectivity to a set of MNs are also the mobility managers for those MNs. In the following we will call these access routers Distributed Anchor Routers (DARs).

The diagram in Figure 1 depicts the operations of the proposed solution. When a mobile node attaches to a distributed anchor router, it gets an IPv6 address which is topologically anchored at the DAR (Pref1::addr1 - HoA1). In the scheme we assume the address configuration takes place through a Router Solicitation/Router Advertisement handshake. While attached to this DAR, the mobile can send and receive traffic using HoA1 without traversing any tunneling nor special packet handling.

If the mobile node moves to a different DAR, it gets a new IPv6 address from the new access router (Pref2::addr2 - HoA2). In case the MN wants to keep the reachability of the IPv6 address(es) it obtained from the previous DAR (note that this decision is dynamic and it is out of scope of this document, it can be done on an application basis for example), the host has to involve its MIPv6 stack, by sending a Binding Update to the DAR where the IPv6 address is anchored, using the address obtained from the current DAR as care-of address (in our example the MN binds HoA2 as CoA to DAR1).
In this way, the IPv6 address that the node wants to maintain in use (Pref1::addr1) plays the role of home address (HoA1), and the DAR from where that address was configured plays the role of Home Agent (for that particular address). In this scenario, old flows are anchored to the previous DAR (DAR1), which is in charge to encapsulate the packets and deliver them to the MN’s CoA. The IP tunnel is bi-directional, so the MN does the same when sending packets with the old address (HoA1). Conversely, new IP flows are started using the address configured at the new DAR (HoA2). These flows are handled by the new DAR as a plain IPv6 router.

Note that the FAMA approach basically enables a mobile node to simultaneously handle several IPv6 addresses -- each of them anchored at a different DAR -- ensuring their continuous reachability by using Mobile IPv6 in a distributed fashion (i.e., each access router is a potential home agent for the address it delegates, if required). Figure 2 illustrates the above case in which the MN is connected to
DAR2, but flow1 is anchored at DAR1, because it was started by the MN using the IPv6 address Pref1::addr1, configured when the MN was connected to DAR1. In the same example, the MN starts flow2 using Pref2::addr2, assigned by DAR2.

```
++---+     +---+
| CN1 |     | CN2 |
+*---+     +*---+
  *     *     *
****     *
flow1 *     * flow2
  *     *     *
  *     *     *
------     ------

| DAR1**(*)--DAR2**---DAR3 |
|    \     \   |
+-----+   \*-----+  \\
  *     *     *
flow1 using \*---+ flow2 using
Pref1::addr1 | *  * | Pref2::addr2
  *MN*       
------
```

Operations sequence                  Packets flow

Figure 2: MN’s flows forwarding in FAMA

The same operations take place if the MN moves to another DAR. The MN obtains a new address (Pref3::addr3 - HoA3), which is indicated as CoA in the BU messages sent by the MN to the previous DARs. This distributed address anchoring is enabled on demand and on a per-address granularity, which means that depending on the user needs, it might be the case that all, some or none of the IPv6 addresses that a mobile node configures while moving within a FAMA domain, are kept reachable and used by the mobile. The scheme in Figure 3 depicts the example where the MN updates all the previous DARs, mapping the corresponding HoA with the new CoA.
In traditional Mobile IPv6, the communication between the MN and the HA is secured through IPsec [RFC4877]. Following a similar approach in FAMA is difficult due to the large number of security associations that would be required, since any gateway of the access network can play the role of home agent for any mobile node. In order to overcome this problem and provide authentication between the DAR and the MNs, we propose the use of Cryptographically Generated Addresses [RFC3972] (CGAs), as introduced in [I-D.laganier-mext-cga]. CGAs are a powerful mechanism allowing authentication of the packets and requires no public-key infrastructure, hence it is well-suited for this application.

Following the ideas presented above, every time an MN attaches to a DAR, it configures a CGA from a prefix anchored at the DAR (e.g., by using stateless address auto-configuration mechanisms). This address
can then be used by the MN to establish a communication with a remote Correspondent Node (CN) while attached to that particular DAR. If the mobile then moves to a new DAR (nDAR), the following two cases are possible: i) there is no need for the address that was configured at the previous DAR (pDAR) to survive the movement: in this case there is no further action required; ii) the mobile wants to keep the reachability of the address configured at pDAR: in this case Mobile IPv6 is triggered, and the MN sends a Binding Update (BU) message to the pDAR, using the address configured at the previous DAR as home address, and the address configured at the new DAR as care-of address. This BU includes the CGA parameters and signature [I-D.laganier-mext-cga], which are used by the receiving DAR to identify the MN as the legitimate owner of the address. Although the use of CGAs does not impose a heavy burden in terms of performance, depending on the number of MNs handled at the DAR, the processing of the CGAs can be problematic. To reduce the complexity of the proposed protocol, we suggest an alternative mechanism to authenticate any subsequent signaling packets exchanged between the MN and the DAR (in case the mobile performs a new attachment to a different DAR). This alternative method relies on the use of a Permanent Home Keygen Token (PHKT), which will be used to generate the Authorization option that the MN has to include in all next Binding Update messages. This token is forwarded to the MN in the Binding Acknowledgment message, sent on reply to the BU. The procedure is depicted in Figure 4. Once the signaling procedure is completed, a bi-directional tunnel is established between the mobile node and the DAR where the IPv6 address is anchored (the "home" DAR -- HDAR -- for that particular address), so the mobile can continue using the IPv6 address.
In case the MN performs any subsequent movements and it requires to maintain the reachability of an address for which it has already sent a BU, the following BU messages can be secured using the PHKT exchanged before, reducing the computational load at the receiving DAR.

Note that on every attachment of a node to a DAR, the terminal also obtains a new IPv6 address which is topologically anchored at that DAR, and that this address can be used for new communications (avoiding in this way the tunneling required when using an address anchored at a different DAR). A mobile can keep multiple IPv6 addresses active and reachable at a given time, and that requires to send -- every time the MN moves -- a BU message to all the previous DARs that are anchoring the IP flows that the MN wish to maintain.

4. IANA Considerations

TBD.

5. Security Considerations

Although the approach documented in this document is attractive for the reduced signaling overhead caused by the mobility support, it can
be misused in some particular scenarios by malicious nodes that wish to export an incorrect CoA in the BU message, since it does provide proof of the MN’s reachability at the visited network. Indeed, the CGA approach assures that the BU message has been sent by the legitimate HoA’s owner but it does not make sure that same MN to be reachable at the CoA indicated. This requires further analysis.

A possible approach to provide a more secure solution is the following: a Return Routability procedure similar to the one defined in MIPv6 Route Optimization can be used to mitigate the aforementioned security issue. The Return Routability procedure starts after the handoff. Instead of sending the BU message, the MN sends a Care-of Test Init message (CoTI). This message is replied by the DAR with a Care-Of Test message containing a CoA Keygen Token. The MN can now send a BU using both Home and CoA Keygen tokens to prove its reachability at both the HoA and the CoA. The message and the knowledge of both tokens is a proof that the MN is the legitimate node who has sent the BU and also is reachable at the CoA indicated. As all security improvements, the one proposed incurs in a performance penalty, in this case an increase in the handover delay. Specifically this enhanced security approach requires four messages to be exchanged between the MN and the DAR instead of the two messages of the original solution. In terms of handover delay, it increases it by a factor of two, as the new solution requires to two Round Trip Times (RTTs) to conclude, instead of one.

6. References

6.1. Normative References


6.2. Informative References


[I-D.ietf-dmm-best-practices-gap-analysis]

[I-D.ietf-dmm-requirements]

[I-D.laganier-mext-cga]

Appendix A. Comparison with Requirement document

In this section we describe how our solution addresses the DMM requirements listed in [I-D.ietf-dmm-requirements].

A.1. Distributed Processing

"IP mobility, network access and routing solutions provided by DMM MUST enable distributed processing for mobility management of some flows so that traffic does not need to traverse centrally deployed mobility anchors and thereby avoid non-optimal routes."

In our solution, a DAR is responsible to handle the mobility for those IP flows started when the MN is attached to it. As long as the MN remains connected to the DAR’s access links, the IP packets of such flows can benefit from the optimal path. When the MN moves to another DAR, the path becomes non-optimal for ongoing flows, as they are anchored to the previous DAR, but newly started IP sessions are forwarded by the new DAR through the optimal path.
A.2. Transparency to Upper Layers when needed

"DMM solutions MUST provide transparent mobility support above the IP layer when needed. Such transparency is needed, for example, when, upon change of point of attachment to the network, an application flow cannot cope with a change in the IP address. However, it is not always necessary to maintain a stable home IP address or prefix for every application or at all times for a mobile node."

Our DMM solution operates at the IP layer, hence upper layers are totally transparent to the mobility operations. In particular, ongoing IP sessions are not disrupted after a change of access network. The routability of the old address is ensured by the IP tunnel with the old DAR. New IP sessions are started with the new address. From the application’s perspective, those processes which sockets are bound to a unique IP address do not suffer any impact. For the other applications, the sockets bound to the old address are preserved, whereas next sockets use the new address.

A.3. IPv6 deployment

"DMM solutions SHOULD target IPv6 as the primary deployment environment and SHOULD NOT be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used."

The DMM solution we propose targets IPv6 only.

A.4. Existing mobility protocols

"A DMM solution SHOULD first consider reusing and extending IETF-standardized protocols before specifying new protocols."

This DMM solution is derived from the operations and messages specified in [RFC6275], [RFC3972], and [I-D.laganier-mext-cga].

A.5. Co-existence with deployed networks and hosts

"The DMM solution MUST be able to co-exist with existing network deployments and end hosts. For example, depending on the environment in which DMM is deployed, DMM solutions may need to be compatible with other deployed mobility protocols or may need to co-exist with a network or mobile hosts/routers that do not support DMM protocols. The mobile node may also move between different access networks, where some of them may support neither DMM nor another mobility protocol. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when allowed by the trust relationship between them."
The proposed solution can provide a fallback mechanism employing legacy Mobile IPv6, for instance forcing the MN to use only one DAR. Moreover, this solution applies when the MN is connected to an administrative domain not supporting trust relationships. Indeed, all the IP sessions can remain anchored to the DARs of the "home" domain. Our solution can be deployed across different domains with trust agreements.

A.6. Security considerations

"DMM protocol solutions MUST consider security risks introduced by DMM into the network. Such considerations may include authentication and authorization mechanisms that allow a mobile host/router to use the mobility support provided by the DMM solution; measures against redirecting traffic to the wrong host when providing DMM support; signaling message protection for authentication, integrity and confidentiality."

The proposed solution uses a CGA-based security system to enable authentication and authorization of mobile hosts.

A.7. Multicast

"DMM SHOULD enable multicast solutions in flexible distribution scenario. This flexibility pertains to the preservation of IP multicast nature from the perspective of a mobility entity and transmission of multicast packets to/from various multicast-enabled entities. Therefore, this flexibility enables different IP multicast flows with respect to a mobile host to be managed (e.g., subscribed, received and/or transmitted) using multiple multicast-enabled endpoints."

This solution does not include multicast traffic in its scope. Nevertheless, it allows combining multicast support solutions, such as local subscription at each DAR, which would result in a flexible distribution scenario.
Authors’ Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid  28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI:   http://www.it.uc3m.es/cjbc/

Antonio de la Oliva
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid  28911
Spain

Phone: +34 91624 8803
Email: aoliva@it.uc3m.es
URI:   http://www.it.uc3m.es/aoliva/

Fabio Giust
Institute IMDEA Networks and Universidad Carlos III de Madrid
Av. del Mar Mediterraneo, 22
Leganes, Madrid  28918
Spain

Email: fabio.giust@imdea.org
Abstract

Distributed Mobility Management solutions allow for setting up networks so that traffic is distributed in an optimal way and does not rely on centralized deployed anchors to provide IP mobility support.

There are many different approaches to address Distributed Mobility Management, as for example extending network-based mobility protocols (like Proxy Mobile IPv6), or client-based mobility protocols (as Mobile IPv6), among others. This document follows the former approach, and proposes a solution based on Proxy Mobile IPv6 in which mobility sessions are anchored at the last IP hop router (called distributed gateway). The distributed gateway is an enhanced access router which is also able to operate as local mobility anchor or mobility access gateway, on a per prefix basis. The draft focuses on the required extensions to effectively support simultaneously anchoring several flows at different distributed gateways.

This draft introduces the concept of distributed logical interface (at the distributed gateway), which is a software construct that allows to easily hide the change of anchor from the mobile node. Additionally, the draft describes how to provide session continuity in inter-domain scenarios in which dynamic tunneling or signaling between distributed gateways from different operators is not allowed.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering
Table of Contents

1. Introduction .................................................. 4
2. Terminology ..................................................... 4
3. Solution’s overview ............................................. 5
4. Simultaneous anchoring of multiple flows (single operator) ... 7
   4.1. The Distributed Logical Interface (DLIF) concept ........ 8
   4.2. D-GW protocol operation .................................. 11
   4.3. Message format ............................................. 14
       4.3.1. Proxy Binding Update .............................. 14
       4.3.2. Proxy Binding Acknowledgment .................... 14
       4.3.3. Anchored Prefix Option ............................ 15
       4.3.4. Local Prefix Option ................................ 16
       4.3.5. DLIF Link-local Address Option .................... 17
       4.3.6. DLIF Link-layer Address Option .................... 18
5. Simultaneous anchoring of multiple flows (multiple operators) .......... 19
6. IANA Considerations .............................................. 21
7. Security Considerations .......................................... 21
8. References ...................................................... 21
   8.1. Normative References .................................... 21
   8.2. Informative References ................................... 22
Appendix A. Implementation experience ............................. 22
Authors’ Addresses ............................................... 23
1. Introduction

The Distributed Mobility Management (DMM) paradigm aims at minimizing the impact of currently standardized mobility management solutions, which are centralized (at least to a considerable extent).

Centralized mobility solutions, such as Mobile IPv6 or the different macro-level mobility management solutions of 3GPP EPS, base their operation on the existence of a central entity (e.g., HA, LMA, PGW or GGSN) that anchors the IP address used by the mobile node and is in charge of coordinating the mobility management (MM) (sometimes helped by a third entity like the MME or the HSS). This central anchor point is in charge of tracking the location of the mobile and redirecting its traffic towards its current topological location. While this way of addressing mobility management has been fully developed by the Mobile IP protocol family and its many extensions, there are also several limitations that have been identified [I-D.chan-distributed-mobility-ps]. Among them, we can just highlight sub-optimal routing, scalability problems (in the network and in the centralized anchor) and reliability [I-D.ietf-dmm-requirements].

Several DMM-based approaches are being proposed and explored now [I-D.ietf-dmm-best-practices-gap-analysis], [commag.dmm-standards]. One of them is based on extending network-based mobility protocols (such as Proxy Mobile IPv6 [RFC5213] or GTP) to operate in distributed fashion. This document proposes a solution that falls in this category, defining a new logical entity, called Distributed Gateway (D-GW) which basically encompasses the functionalities of plain IPv6 access router, MAG and LMA, on a per-IPv6 prefix basis. The main contribution of this draft is the definition of the mechanisms required to support the operation of such a network-based mobility solution when several flows are simultaneously anchored at different D-GWs, by introducing the concept of Distributed Logical Interface (DLIF). The document also defines the required PMIPv6 signaling extensions. Last, but not least, the solution is also extended to provide session continuity across different domains.

2. Terminology

The following terms used in this document are defined in the Proxy Mobile IPv6 specification [RFC5213]:

- Local Mobility Anchor (LMA)
- Mobile Access Gateway (MAG)
Mobile Node (MN)

Binding Cache Entry (BCE)

Proxy Care-of Address (P-CoA)

Proxy Binding Update (PBU)

Proxy Binding Acknowledgment (PBA)

The following terms are defined and/or used in this document:

D-GW (Distributed Gateway). First IP hop router used by the mobile
node. It provides an IPv6 prefix (topologically anchored at the
D-GW) to each attaching mobile node.

Anchoring D-GW. A previously visited D-GW anchoring an IPv6 prefix
which is still used by a mobile node.

Serving D-GW. The D-GW the MN is currently attached to.

DLIF (Distributed Logical Interface). It is a logical interface at
the IP stack of the D-GW. For each active prefix used by the
mobile node, the serving D-GW has a DLIF configured (associated to
the anchoring D-GW). In this way, a serving D-GW exposes itself
towards each MN as multiple routers, one per active anchoring
D-GW.

HSS (Home Subscriber Server). In a 3GPP architecture, it is the
master user database that contains the subscription-related
information (subscriber profiles), performs authentication and
authorization of the user, and can provide information about the
subscriber’s location and IP information.

3. Solution’s overview

A new logical network entity, called Distributed Gateway (D-GW) is
introduced at the edge of the network, close to the MN. It
implements the functionality of a plain IPv6 access router (AR), a
mobile access gateway (MAG) and a local mobility anchor (LMA), on a
per-MN and per-IPv6-prefix, as described later.

The solution basically extends Proxy Mobile IPv6 [RFC5213] to behave
in a distributed fashion, similarly as what has been proposed in
[I-D.seite-dmm-dma] and [I-D.bernardos-dmm-pmip]. This is achieved
by the D-GW logically behaving as a distributed mobility anchor,
which comprises the following:
When a mobile node attaches to a D-GW (initial attachment or handover), the D-GW provides an IPv6 prefix to the MN, acting as a regular IPv6 router (with the only difference that the delegated prefix is only assigned to one single MN, not being shared with any other node). The D-GW that the mobile node is currently attached to is called "serving D-GW".

When a mobile node performs a handover, it attaches to a new D-GW and configures a new IPv6 address out of the prefix provided and anchored by the new serving D-GW. As before, the serving D-GW behaves as a plain IPv6 router for that particular MN and the delegated (locally anchored) prefix. If the MN has active traffic using addresses anchored by other D-GWs (which are called "anchoring D-GWs") or it just needs to keep the reachability of these addresses, the current serving D-GW also acts as MAG, by sending the required proxy binding update (PBU) to the corresponding anchoring D-GWs. The anchoring D-GWs therefore behave as LMA for this particular MN and the IPv6 prefixes they are anchoring, replying with a PBA.

Once the PBU/PBA signaling is completed, a bidirectional tunnel is established between the serving D-GW and the anchoring D-GW (one per D-GW anchoring an active prefix used by the MN). These tunnels are used to provide IP address continuity to prefixes that are not anchored at the serving D-GW.

The means for a serving D-GW to obtain the information about the prefixes that a locally attached mobile node wants to keep reachable, and the associated anchoring D-GWs are out of the scope of this draft. Among the possible mechanisms that can be used to let the D-GW know about the prefixes that should be kept reachable, we can cite for instance layer-2 triggers/signaling. Regarding the mapping of IPv6 prefixes to anchoring D-GWs, there might be either fully distributed mechanisms in place, or the information can be maintained in a centralized repository (e.g., in the HSS, using a centralized LMA [I-D.bernardos-dmm-pmip], etc.).

The basic operation of the solution is shown with an example in Figure 1. MN1 attaches to D-GW1 (thus becoming its serving D-GW) and configures an IPv6 address (prefA::MN1) out of a prefix locally anchored at D-GW1 (prefA::/64). At this point, MN1 can communicate with any correspondent node of the Internet, being the traffic anchored at D-GW1. If later on MN1 moves to D-GW2, a new IPv6 address (PrefB::MN1) is configured by the mobile node, this time out of prefB::/64, which is anchored at D-GW2 (which becomes the new serving D-GW). D-GW2 also exchanges the required PBU/PBA signaling to ensure that data traffic using prefA::MN1 still reaches the mobile node.
node, by setting up a bidirectional tunnel between D-GW1 (anchoring D-GW) and D-GW2 (serving D-GW).

![Diagram of basic operation of the solution]

**Figure 1: Basic operation of the solution**

The next sections of this draft focus on the detailed operation of the D-GWs when a mobile node has multiple flows anchored at different distributed gateways.

4. Simultaneous anchoring of multiple flows (single operator)

In this section we describe the mechanisms required in the network to enable simultaneous anchoring of several flows at different D-GWs within the same operator.
4.1. The Distributed Logical Interface (DLIF) concept

One of the main challenges of a network-based DMM solution is how to allow a mobile node to simultaneously send/receive traffic which is anchored at different D-GWs, and how to influence on the preference of the mobile selecting the source IPv6 address for a new communication, without requiring special support on the mobile node stack. This document defines the Distributed Logical Interface (DLIF), which is a software construct that allows to easily hide the change of anchor from the mobile node.

The basic idea of the DLIF concept is the following. Each serving D-GW exposes itself towards a given MN as multiple routers, one per active anchoring D-GW associated to the MN. Let's consider the example shown in Figure 2, MN1 initially attaches to D-GW1, configuring an IPv6 address (prefA::MN1) from a prefix locally anchored at D-GW1 (prefA::/64). At this stage, D-GW1 plays both the role of anchoring and serving D-GW, and also it behaves as a plain IPv6 access router. D-GW1 creates a distributed logical interface to communicate (point-to-point link) with MN1, exposing itself as a (logical) router with a specific MAC (e.g., 00:11:22:33:01:01) and IPv6 addresses (e.g., prefA::DGW1/64 and fe80:211:22ff:fe33:101/64) and additional IPv6 prefixes (e.g., prefA::/64 with AdvPrefLft=0).

Figure 2: DLIF: exposing multiple routers (one per active anchoring D-GW)
using the DLIF mn1dgw1. As explained below, these addresses represent the "logical" identity of D-GW towards MN, and will "follow" the mobile node while roaming within the domain (note that the place where all this information is maintained and updated is out-of-scope of this draft; potential examples are to keep it on the HSS or the user’s profile).

If MN moves and attaches to a different D-GW of the domain (D-GW2 in the example of Figure 2), this D-GW will create a new logical interface (mn1dgw2) to expose itself towards MN, providing it with a locally anchored prefix (prefB::/64). In this case, since the MN has another active IPv6 address anchored at a D-GW, D-GW2 also needs to create an additional logical interface configured to exactly resemble the one used by D-GW to communicate with MN. In this example, there is only one active anchoring D-GW (in addition to D-GW2, which is the serving one): D-GW1, so only the logical interface mn1dgw1 is created, but the same process would be repeated in case there were more active anchoring D-GWs involved. In order to maintain the prefix anchored at D-GW1 reachable, a tunnel between D-GW1 and D-GW2 is established and the routing is modified accordingly. The PBU/PBA signaling is used to set-up the bi-directional tunnel between D-GW1 and D-GW2, and it might also be used to convey to D-GW2 the information about the prefix(es) anchored at D-GW1 and about the addresses of the associated DLIF (i.e., mn1dgw1).

![Distributed Logical Interface concept](image)

**Figure 3: Distributed Logical Interface concept**
Figure 3 shows the logical interface concept in more detail. The figure shows two D-GWs and three MNs. D-GW1 is currently serving MN2 and MN3, while D-GW2 is serving MN1. MN1, MN2 and MN3 have two active anchoring D-GWs: D-GW1 and D-GW2. Note that a serving D-GW always plays the role of anchoring D-GW for the attached (served) MNs. Each D-GW has one single physical wireless interface.

As introduced before, each MN always "sees" multiple logical routers -- one per active anchoring D-GW -- independently of to which serving D-GW the MN is currently attached. From the point of view of the MN, these D-GWs are portrayed as different routers, although the MN is physically attached to one single interface. The way this is achieved is by the serving D-GW configuring different logical interfaces. If we focus on MN1, it is currently attached to D-GW2 (i.e., D-GW2 is its serving D-GW) and, therefore, it has configured an IPv6 address from D-GW2's pool (e.g., prefB::/64). D-GW2 has set-up a logical interface (mn1dgw2) on top of its wireless physical interface (phy if D-GW2) which is used to serve MN1. This interface has a logical MAC address (LMAC6), different from the hardware MAC address (HMAC2) of the physical interface of D-GW2. Over the mn1dgw2 interface, D-GW2 advertises its locally anchored prefix prefB::/64. Before attaching to D-GW2, MN1 visited D-GW1, configuring also an address locally anchored at this D-GW, which is still being used by the MN1 in active communications. MN1 keeps "seeing" an interface connecting to D-GW1, as if it were directly connected to the two D-GWs. This is achieved by the serving D-GW (D-GW1) configuring an additional distributed logical interface: mn1dgw1, which behaves exactly as the logical interface configured by the actual D-GW1 when MN1 was attached to it. This means that both the MAC and IPv6 addresses configured on this logical interface remain the same regardless of the physical D-GW which is serving the MN. The information required by a serving D-GW to properly configure this logical interfaces can be obtained in different ways: as part of the information conveyed in the PBA, from an external database (e.g., the HSS) or by other means. As shown in the figure, each D-GW may have several logical interfaces associated to each attached MN, having always at least one (since a serving D-GW is also an anchoring D-GW for the attached MN).

In order to enforce the use of the prefix locally anchored at the serving D-GW, the router advertisements sent over those logical interfaces playing the role of anchoring D-GWs (different from the serving one) include a zero prefix lifetime. The goal is to deprecate the prefixes delegated by these D-GWs (which will be no longer serving the MN). Note that on-going communications keep on using those addresses, even if they are deprecated, so this only affects to new sessions.
The distributed logical interface concept also enables the following use case. Suppose that access to a local IP network is provided by a given D-GW (e.g., D-GW1 in the example shown in Figure 2) and that the resources available at that network cannot be reached from outside the local network (e.g., cannot be accessed by an MN attached to D-GW2). This is similar to the LIPA scenario currently being considered by 3GPP. The goal is to allow an MN to be able to roam while still being able to have connectivity to this local IP network. The solution adopted to support this case makes use of RFC 4191 [RFC4191] more specific routes when the MN moves to a D-GW different from the one providing access to the local IP network (D-GW1 in the example). These routes are advertised through the distributed logical interface representing the D-GW providing access to the local network (D-GW1 in this example). In this way, if MN1 moves from D-GW1 to D-GW2, any active session that MN1 may have with a node of the local network connected to D-GW1 will survive, being the traffic forwarded via the tunnel between D-GW1 and D-GW2. Also, any potential future connection attempt towards the local network will be supported, even though MN1 is no longer attached to D-GW1.

4.2. D-GW protocol operation

This section describes the D-GW operation in more detail.

Figure 4 shows an example of the D-GW operation:

1. MN1 attaches to D-GW1. This event is detected by D-GW1 (based on layer 2 signaling/triggers or the reception of a Router Solicitation sent by MN1).

2. An IPv6 prefix from the pool of locally anchored prefixes is selected by D-GW1 to be delegated to MN1 (prefA::/64). D-GW1 sets up a distributed logical interface aimed at interfacing with MN1, called mn1dgw1. D-GW1 starts sending router advertisements to MN1, including the delegated prefix.

3. D-GW1 learns if it is an attachment due to a handover (how this is done is out-of-scope of this draft). In this case it is an initial attachment, so nothing else is required.

4. The DLIF mn1dgw1 is used by D-GW1 to advertise the locally anchored prefix (prefA::/64) to MN1. Using this prefix, MN1 configures an IPv6 address (prefA::MN1/64) that can be used to start new sessions (which will be anchored at D-GW1). Traffic using the address prefA::MN1 is received at the interface mn1dgw1 and directly forwarded by D-GW1 towards its destination. Traffic between MN1 and the local network reachable via D-GW1 (localnet) is handled normally by D-GW1 (as MN1 is locally attached).
5. MN1 performs a handover to D-GW2. This event is detected by D-GW2.

6. An IPv6 prefix from the pool of locally anchored prefixes is selected by D-GW2 to be delegated to MN1 (prefB::/64). D-GW2 sets up a distributed logical interface aimed at interfacing with MN1, called mn1dgw2. D-GW2 starts sending router advertisements to MN1, including the delegated prefix. Traffic using the address prefB::MN1 is received at the interface mn1dgw2 and directly forwarded by D-GW2 towards its destination.

7. D-GW2 learns that this is a handover of MN1, and that it previously visited D-GW1. D-GW2 sends a PBU to D-GW1, which replies with a PBA. This PBA MAY include information about the prefix(es) anchored at D-GW1, the parameters needed by D-GW2 to set-up the DLIF mn1dgw1, and the prefixes of local networks reachable via D-GW (if any). Alternatively, this information MAY be obtained using a different approach (such as storing it in the HSS or some other external repository). A bi-directional tunnel between D-GW1 and D-GW2 is set-up, as well as the required routing entries.

8. D-GW2 sets up the DLIF mn1dgw1, aimed at "logically" resembling D-GW1, so MN1 does not detect any change at layer-3. D-GW2 starts sending router advertisements to MN1 through mn1dgw2, which include the prefix anchored at D-GW1 (prefA::/64) with zero lifetime to deprecate the prefix (or alternatively it MAY include a low Default Router Preference [RFC4191] if communication to this D-GW is still needed in the future). In this way, prefA::MN1 is not preferred for new communications. The RAs MAY also include a Route Information Option (RIO) [RFC4191] with the prefix of localnet, which is the network that is only locally reachable via D-GW1 (e.g., as in the LIPA scenarios considered by the 3GPP), so MN1 picks D-GW1 (the "logical" version of it portrayed by D-GW2) when sending traffic to that network, including the delegated prefix. Traffic using the address prefA::MN1 is received at the interface mn1dgw1 and forwarded via the tunnel with D-GW1, which then forwards it towards its destination. Traffic between MN1 and the network locally reachable via D-GW1 (localnet) is also handled via mn1dgw1 and sent through the tunnel.
Figure 4: D-GW protocol operation

attachment

configures prefA::MN1

set-up of new RA@mn1dgw1
(prefA::/64)

(traffic using prefA::MN1)

(traffic with local net)

handover

configures prefB::MN1
and keeps using prefA::MN1

PBU

set-up tunnel

set-up of tunnel & DLIF mn1dgw1

RA@mn1dgw2

DLIF: mn1dgw2

(prefB::/64)

PBA(mn1dgw1, prefA::/64, preflocalnet)

(prefA::/64, lft=0, RIO: preflocalnet)

(prefA::/64)

(traffic using prefA::MN1)

(traffic using prefB::MN1)

(traffic with local net)
4.3. Message format

This section defines extensions to the Proxy Mobile IPv6 [RFC5213] protocol messages.

4.3.1. Proxy Binding Update

A new flag (D) is included in the Proxy Binding Update to indicate that the Proxy Binding Update is coming from a Distributed Gateway and not from a mobile access gateway. The rest of the Proxy Binding Update format remains the same as defined in [RFC5213].

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Sequence #         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|A|H|L|K|M|R|P|D| Reserved      |            Lifetime           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
| Mobility options                       |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Distributed Gateway Flag (D)

The Distributed Gateway Flag is set to indicate to the receiver of the message that the Proxy Binding Update is from a Distributed Gateway.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2 of [RFC6275]. The distributed gateway MUST ignore and skip any options that it does not understand.

4.3.2. Proxy Binding Acknowledgment

A new flag (D) is included in the Proxy Binding Acknowledgment to indicate that the sender supports operating as a distributed gateway. The rest of the Proxy Binding Acknowledgment format remains the same as defined in [RFC5213].
Distributed Gateway Flag (D)

The Distributed Gateway Flag is set to indicate that the sender of the message supports operating as a distributed gateway.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2 of [RFC6275]. The distributed gateway MUST ignore and skip any options that it does not understand.

4.3.3. Anchored Prefix Option

A new Anchored Prefix option is defined for use with the Proxy Binding Update and Proxy Binding Acknowledgment messages exchanged between distributed gateways. This option is used for exchanging the mobile node’s prefix anchored at the anchoring D-GW. There can be multiple Anchored Prefix options present in the message.

The Anchored Prefix Option has an alignment requirement of 8n+4. Its format is as follows:
**Type**

To be assigned by IANA.

**Length**

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields. This field MUST be set to 18.

**Reserved**

This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

**Prefix Length**

8-bit unsigned integer indicating the prefix length of the IPv6 prefix contained in the option.

**Anchored Prefix**

A sixteen-byte field containing the mobile node’s IPv6 Anchored Prefix.

### 4.3.4. Local Prefix Option

A new Local Prefix option is defined for use with the Proxy Binding Update and Proxy Binding Acknowledgment messages exchanged between distributed gateways. This option is used for exchanging a prefix of a local network that is only reachable via the anchoring D-GW. There can be multiple Local Prefix options present in the message.

The Local Prefix Option has an alignment requirement of 8n+4. Its
format is as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Reserved</th>
<th>Prefix Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type
To be assigned by IANA.

Length
8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields. This field MUST be set to 18.

Reserved
This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Prefix Length
8-bit unsigned integer indicating the prefix length of the IPv6 prefix contained in the option.

Local Prefix
A sixteen-byte field containing the IPv6 Local Prefix.

4.3.5. DLIF Link-local Address Option

A new DLIF Link-local Address option is defined for use with the Proxy Binding Update and Proxy Binding Acknowledgment messages exchanged between distributed gateways. This option is used for exchanging the link-local address of the DLIF to be configured on the serving D-GW so it resembles the DLIF configured on the anchoring D-GW.
The DLIF Link-local Address option has an alignment requirement of 8n+6. Its format is as follows:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-------------------------------+-------------------------------+
| Type | Length |
+-------------------------------+-------------------------------+
| +                                            +
| + DLIF Link-local Address +
| +                                            +
| +                                            +
+-------------------------------+-------------------------------+
```

Type
To be assigned by IANA.

Length
8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields. This field MUST be set to 16.

DLIF Link-local Address
A sixteen-byte field containing the link-local address of the logical interface.

4.3.6. DLIF Link-layer Address Option
A new DLIF Link-layer Address option is defined for use with the Proxy Binding Update and Proxy Binding Acknowledgment messages exchanged between distributed gateways. This option is used for exchanging the link-layer address of the DLIF to be configured on the serving D-GW so it resembles the DLIF configured on the anchoring D-GW.

The format of the DLIF Link-layer Address option is shown below. Based on the size of the address, the option MUST be aligned appropriately, as per mobility option alignment requirements specified in [RFC6275].
Type
To be assigned by IANA.

Length
8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields.

Reserved
This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

DLIF Link-layer Address
A variable length field containing the link-layer address of the logical interface to be configured on the serving distributed gateway.

The content and format of this field (including byte and bit ordering) is as specified in Section 4.6 of [RFC4861] for carrying link-layer addresses. On certain access links, where the link-layer address is not used or cannot be determined, this option cannot be used.

5. Simultaneous anchoring of multiple flows (multiple operators)
An MN may roam between D-GWs that do not belong to the same operator, and therefore might end up having multiple simultaneous flows, anchored at different operators. Since dynamically setting up tunnels between different operators (i.e., between D-GWs belonging to different operators) is usually not supported, a solution should be devised to ensure session continuity in this scenario, even if it is at the cost of a sub-optimal routing.
In this section we describe the required extensions to support inter-domain operation. The basic solution consists in using a centralized LMA (usually located in the home domain) as top-level anchor to guarantee session continuity when crossing operator borders. We assume that the necessary roaming agreements are in place in order to support setting up tunnels between the LMA located at the home domain of the MN and the visited D-GWs.

Figure 5: Simultaneous anchoring of multiple flows across multiple operators

Figure 5 shows an example of the inter-domain operation. MN1 initially attaches to D-GW1 (which belongs to OperatorA), and configures prefA::MN1 address out of one prefix anchored at D-GW1 (prefA::/64). If MN1 moves to D-GW2, which is managed by OperatorB, tunnels need to be established via the centralized LMA at the MN1’s operators core, since we assume that no direct tunneling is possible between D-GWs belonging to different operators. In this case, D-GW3
establishes one tunnel with the centralized LMA to send/receive traffic using prefA::/64. From the point of view of D-GW2, the operation is just as if the LMA was the D-GW anchoring this prefix. Analogously, the LMA establishes one tunnel with D-GW1 (from the point of view of D-GW1, the LMA is the current serving D-GW of MN1). Regarding the signaling, it is similar to the intra-operator scenario, though in this case the PBU/PBA sequence is performed twice, once between D-GW2 and the LMA, and another one between the LMA and D-GW1 (i.e., because two different tunnels are created).

6. IANA Considerations

This document defines new mobility options that require IANA actions.

7. Security Considerations

The protocol extensions defined in this document share the same security concerns of Proxy Mobile IPv6 [RFC5213]. It is recommended that the signaling messages, Proxy Binding Update and Proxy Binding Acknowledgment, exchanged between the distributed gateways, or between a distributed gateway and a centralized local mobility anchor, are protected using IPsec using the established security association between them. This essentially eliminates the threats related to the impersonation of a distributed gateway or the local mobility anchor.

8. References

8.1. Normative References


8.2. Informative References

[I-D.bernardos-dmm-pmip]

[I-D.chan-distributed-mobility-ps]

[I-D.ietf-dmm-best-practices-gap-analysis]

[I-D.ietf-dmm-requirements]

[I-D.seite-dmm-dma]

[commag.dmm-standards]

Appendix A. Implementation experience

The DLIF concept can be easily implemented using features that are usually available on several OSs. Among the possible mechanisms that can be used to do it, the Linux macvlan support allows the creation of different logical interfaces over the same physical one. Each logical interface appears as a regular interface to the Linux OS (which can be configured normally), and it supports configuring the MAC address exposed by the logical interface. The destination MAC
address is used by the OS to decide which logical interface (configured on top of a physical interface) is in charge of processing an incoming L2 frame.

The EU FP7 MEDIEVAL project implemented a prototype of the DLIF concept using the Linux macvlan support, the radvd daemon, the Linux Advanced Routing and Traffic Control features and the standard iproute2 collection of utilities:

- The macvlan support enables iproute2 tools to be able to create, destroy and configure DLIFs on demand over a single physical interface. One of the important features that needs to be configured is the logical MAC address exposed by the DLIF, as well as the IPv6 addresses, as they should remain the same regardless of the serving D-GW where the DLIF is configured.

- Since the distributed logical interfaces created using the macvlan support appear as regular network interfaces, they can be used normally in the radvd configuration file. Then, by dynamically modifying the radvd configuration file and reloading it, we can control the router advertisements sent to each MN (e.g., advertizing new IPv6 prefixes, deprecating prefixes anchored at other serving D-GWs, announcing RFC 4191 specific routes or changing router preferences).

- Each time a DLIF is created, it is also needed to properly configure source-based IPv6 routes, as well as tunnels (in case of handover). This is supported by the Linux Advanced Routing and Traffic Control features.

- Last, but not least, current Linux kernels support the configuration of RFC 4191 specific routes (by processing Route Information Options contained in RAs). The kernel support can be easily enabled by using the net.conf.ipv6.*.accept_ra_rt_info_max_plen kernel configuration parameter.

- A prototype implementation of the solution described in this document, together with the solution specified in [I-D.bernardos-dmm-pmip] was shown during IETF 83rd, in Paris in March 2012.
Authors’ Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain
Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Juan Carlos Zuniga
InterDigital Communications, LLC
1000 Sherbrooke Street West, 10th floor
Montreal, Quebec H3A 3G4
Canada
Email: JuanCarlos.Zuniga@InterDigital.com
URI: http://www.InterDigital.com/
A PMIPv6-based solution for Distributed Mobility Management
draft-bernardos-dmm-pmip-03

Abstract

The number of mobile users and their traffic demand is expected to be ever-increasing in future years, and this growth can represent a limitation for deploying current mobility management schemes that are intrinsically centralized, e.g., Mobile IPv6 and Proxy Mobile IPv6. For this reason it has been waved a need for distributed and dynamic mobility management approaches, with the objective of reducing operators’ burdens, evolving to a cheaper and more efficient architecture.

This draft describes multiple solutions for network-based distributed mobility management inspired by the well known Proxy Mobile IPv6.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 12, 2014.
1. Introduction
Current IP mobility solutions, standardized with the names of Mobile IPv6 [RFC6275], or Proxy Mobile IPv6 [RFC5213], just to cite the two most relevant examples, offer mobility support at the cost of handling operations at a cardinal point, the mobility anchor, and burdening it with data forwarding and control mechanisms for a great amount of users. As stated in [I-D.ietf-dmm-requirements], centralized mobility solutions are prone to several problems and limitations: longer (sub-optimal) routing paths, scalability problems, signaling overhead (and most likely a longer associated handover latency), more complex network deployment, higher vulnerability due to the existence of a potential single point of failure, and lack of granularity on the mobility management service (i.e., mobility is offered on a per-node basis, not being possible to define finer granularity policies, as for example per-application).

The purpose of Distributed Mobility Management is to overcome the limitations of the traditional centralized mobility management [I-D.ietf-dmm-requirements] [I-D.ietf-dmm-best-practices-gap-analysis]; the main concept behind DMM solutions is indeed bringing the mobility anchor closer to the MN. Following this idea, in our proposal, the central anchor is moved to the edge of the network, being deployed in the default gateway of the mobile node. That is, the first elements that provide IP connectivity to a set of MNs are also the mobility managers for those MNs. In the following, we will call these entities Mobility Anchor and Access Routers (MAARs).

This document focuses on network-based DMM, hence the starting point is making PMIPv6 working in a distributed manner [I-D.ietf-dmm-best-practices-gap-analysis]. In our proposal, as in PMIPv6, mobility is handled by the network without the MNs involvement, but, differently from PMIP, when the MN moves from one access network to another, it also changes anchor router, hence requiring signaling between the anchors to retrieve the MN’s previous location(s). Also, a key-aspect of network-based DMM, is that a prefix pool belongs exclusively to each MAAR, in the sense that those prefixes are assigned by the MAAR to the MNs attached to it, and they are routable at that MAAR.

In the following, we consider two main approaches to design our DMM solutions:

- Partially distributed schemes, where the data plane only is distributed among access routers similar to MAGs, whereas the control plane is kept centralized towards a cardinal node used as information store, but relieved from any route management and MN’s data forwarding task.
2. Terminology

The following terms used in this document are defined in the Proxy Mobile IPv6 specification [RFC5213]:

- Local Mobility Anchor (LMA)
- Mobile Access Gateway (MAG)
- Mobile Node (MN)
- Binding Cache Entry (BCE)
- Proxy Care-of Address (P-CoA)
- Proxy Binding Update (PBU)
- Proxy Binding Acknowledgement (PBA)

The following terms are defined and used in this document:

- MAAR (Mobility Anchor and Access Router). First hop router where the mobile nodes attach to. It also plays the role of mobility manager for the IPv6 prefixes it anchors, running the functionalities of PMIP’s MAG and LMA.

- CMD (Central Mobility Database). Node that stores the BCEs allocated for the MNs in the mobility domain.

- P-MAAR (Previous MAAR). MAAR which was previously visited by the MN and is still involved in an active flow using an IPv6 prefix it has advertised to the MN (i.e., MAAR where that IPv6 prefix is anchored). There might be multiple P-MAARs for an MN’s mobility session.

- S-MAAR (Serving MAAR). MAAR which the MN is currently attached to.

3. Partially distributed solution
The following solution consists in de-coupling the entities that participate in the data and the control planes: the data plane becomes distributed and managed by the MAARs near the edge of the network, while the control plane, besides on the MAARs, relies on a central entity called Central Mobility Database (CMD). In the proposed architecture, the hierarchy present in PMIP between LMA and MAG is preserved, but with the following substantial variations:

- The LMA is relieved from the data forwarding role, only the Binding Cache and its management operations are maintained. Hence the LMA is renamed into Central Mobility Database (CMD). Also, the CMD is able to send and parse both PBU and PBA messages.

- The MAG is enriched with the LMA functionalities, hence the name Mobility Anchor and Access Router (MAAR). It maintains a local Binding Cache for the MNs that are attached to it and it is able to send and parse PBU and PBA messages.

- The binding cache will have to be extended to include information regarding previous MAARs where the mobile node was anchored and still retains active data sessions, see Appendix B for further details.

- Each MAAR has a unique set of global prefixes (which are configurable), that can be allocated by the MAAR to the MNs, but must be exclusive to that MAAR, i.e. no other MAAR can allocate the same prefixes.

The MAARs leverage on the Central Mobility Database (CMD) to access and update information related to the MNs, stored as mobility sessions; hence, a centralized node maintains a global view on the status of the network. The CMD is queried whenever a MN is detected to join/leave the mobility domain. It might be a fresh attachment, a detachment or a handover, but as MAARs are not aware of past information related to a mobility session, they contact the CMD to retrieve the data of interest and eventually take the appropriate action. The procedure adopted for the query and the messages exchange sequence might vary to optimize the update latency and/or the signaling overhead. Here is presented one method for the initial registration, and three different approaches to update the mobility sessions using PBUs and PBAs. Each approach assigns a different role to the CMD:

- The CMD is a PBU/PBA relay;

- The CMD is only a MAAR locator;

- The CMD is a PBU/PBA proxy.
3.1. Initial registration

Upon the MN’s attachment to a MAAR, say MAAR1, if the MN is authorized for the service, an IPv6 global prefix belonging to the MAAR’s prefix pool is reserved for it (Pref1) into a temporal Binding Cache Entry (BCE) allocated locally. The prefix is sent in a [RFC5213] PBU with the MN’s Identifier (MN-ID) to the CMD, which, since the session is new, stores a permanent BCE containing as main fields the MN-ID, the MN’s prefix and MAAR1’s address as Proxy-CoA. The CMD replies to MAAR1 with a PBA including the usual options defined in PMIP/RFC5213, meaning that the MN’s registration is fresh and no past status is available. MAAR1 definitely stores the temporal BCE previously allocated and unicasts a Router Advertisement (RA) to the MN including the prefix reserved before, that can be used by the MN to configure an IPv6 address (e.g., with stateless auto-configuration). The address is routable at the MAAR, in the sense that it is on the path of packets addressed to the MN. Moreover, the MAAR acts as plain router for those packets, as no encapsulation nor special handling takes place. Figure 1 illustrates this scenario.

![Diagram of initial registration process]

Operations sequence

Packets flow

Figure 1: First attachment to the network

3.2. The CMD as PBU/PBA relay
When the MN moves from its current access and associates to MAAR2 (now the S-MAAR), MAAR2 reserves another IPv6 prefix (Pref2), it stores a temporal BCE, and it sends a plain PBU to the CMD for registration. Upon PBU reception and BC lookup, the CMD retrieves an already existing entry for the MN, binding the MN-ID to its former location; thus, the CMD forwards the PBU to the MAAR indicated as Proxy CoA (MAAR1), including a new mobility option to communicate the S-MAAR’s global address to MAAR1, defined as Serving MAAR Option in Section 3.6.2. The CMD updates the P-CoA field in the BCE related to the MN with the S-MAAR’s address.

Upon PBU reception, MAAR1 can install a tunnel on its side towards MAAR2 and the related routes for Pref1. Then MAAR1 replies to the CMD with a PBA (including the option mentioned before) to ensure that the new location has successfully changed, containing the prefix anchored at MAAR1 in the Home Network Prefix option. The CMD, after receiving the PBA, updates the BCE populating an instance of the P-MAAR list. The P-MAAR list is an additional field on the BCE that contains an element for each P-MAAR involved in the MN’s mobility session. The list element contains the P-MAAR’s global address and the prefix it has delegated (see Appendix B for further details).

Also, the CMD send a PBA to the new S-MAAR, containing the previous Proxy-CoA and the prefix anchored to it embedded into a new mobility option called Previous MAAR Option (defined in Section 3.6.1), so that, upon PBA arrival, a bi-directional tunnel can be established between the two MAARs and new routes are set appropriately to recover the IP flow(s) carrying Pref1.

Now packets destined to Pref1 are first received by MAAR1, encapsulated into the tunnel and forwarded to MAAR2, which finally delivers them to their destination. In uplink, when the MN transmits packets using Pref1 as source address, they are sent to MAAR2, as it is MN’s new default gateway, then tunneled to MAAR1 which routes them towards the next hop to destination. Conversely, packets carrying Pref2 are routed by MAAR2 without any special packet handling both for uplink and downlink. The procedure is depicted in Figure 2.
For next MN’s movements the process is repeated except for the number of P-MAARs involved, that rises accordingly to the number of prefixes that the MN wishes to maintain. Indeed, once the CMD receives the first PBU from the new S-MAAR, it forwards copies of the PBU to all the P-MAARs indicated in the BCE as current P-CoA (i.e., the MAAR prior to handover) and in the P-MAARs list. They reply with a PBA to the CMD, which aggregates them into a single one to notify the S-MAAR, that finally can establish the tunnels with the P-MAARs.

It should be noted that this design separates the mobility management at the prefix granularity, and it can be tuned in order to erase old mobility sessions when not required, while the MN is reachable through the latest prefix acquired. Moreover, the latency associated to the mobility update is bound to the PBA sent by the furthest P-MAAR, in terms of RTT, that takes the longest time to reach the CMD. The drawback can be mitigated introducing a timeout at the CMD, by which, after its expiration, all the PBAs so far collected are transmitted, and the remaining are sent later upon their arrival.

### 3.3. The CMD as MAAR locator

The handover latency experienced in the approach shown before can be reduced if the P-MAARs are allowed to signal directly their information to the new S-MAAR. This procedure reflect what was described in Section 3.2 up to the moment the P-MAAR receives the PBU with the P-MAAR option. At that point a P-MAAR is aware of the new MN’s location (because of the S-MAAR’s address in the S-MAAR option), and, besides sending a PBA to the CMD, it also sends a PBA to the S-MAAR including the prefix it is anchoring. This latter PBA does not need to include new options, as the prefix is embedded in the HNP option and the P-MAAR’s address OS taken from the message’s source address. The CMD is relieved from forwarding the PBA to the S-MAAR,
as the latter receives a copy directly from the P-MAAR with the necessary information to build the tunnels and set the appropriate routes. In Figure 3 is illustrated the new messages sequence, while the data forwarding is unaltered.

3.4. The CMD as MAAR proxy

A further enhancement of previous solutions can be achieved when the CMD sends the PBA to the new S-MAAR before notifying the P-MAARs of the location change. Indeed, when the CMD receives the PBU for the new registration, it is already in possess of all the information that the new S-MAAR requires to set up the tunnels and the routes. Thus the PBA is sent to the S-MAAR immediately after a PBU is received, including also in this case the P-MAAR option. In parallel, a PBU is sent by the CMD to the P-MAARs containing the S-MAAR option, to notify them about the new MN's location, so they receive the information to establish the tunnels and routes on their side. When P-MAARs complete the update, they send a PBA to the CMD to indicate that the operation is concluded and the information are updated in all network nodes. This procedure is obtained from the first one re-arranging the order of the messages, but the parameters
communicated are the same. This scheme is depicted in Figure 4, where, again, the data forwarding is kept untouched.

```
| MAAR1 | CMD | MAAR2 |
+-------+-----+-------+
| +-----+-----+-----+ +-----+-----+ +-----+
|       | MN   |       |
|       | *    |       |
|       | *    | *    |
|       | *    | *    |
|       | MN   |       |
|       | *    | *    |
|       | *    | *    |
|       | *    | *    |
|       | *    | *    |
```

```
| CN    | +-----+ +-----+ |
|       |       |       |
|       |       |       |
|       |       |       |
|       |       |       |
```

Figure 4: Scenario after a handover, CMD as proxy

3.5. De-registration

The de-registration mechanism devised for PMIPv6 is no longer valid in the Partial DMM architecture. This is motivated by the fact that each MAAR handles an independent mobility session (i.e., a single or a set of prefixes) for a given MN, whereas the aggregated session is stored at the CMD. Indeed, when a previous MAAR initiates a de-registration procedure, because the MN is no longer present on the MAAR’s access link, it removes the routing state for that (those) prefix(es), that would be deleted by the CMD as well, hence defeating any prefix continuity attempt. The simplest approach to overcome this limitation is to deny an old MAAR to de-register a prefix, that is, allowing only a serving MAAR to de-register the whole MN session. This can be achieved by first removing any layer-2 detachment event, so that de-registration is triggered only when the session lifetime expires, hence providing a guard interval for the MN to connect to a new MAAR. Then, a change in the MAAR operations is required, and at this stage two possible solutions can be deployed:
A previous MAAR stops the BCE timer upon receiving a PBU from the CMD containing a "Serving MAAR" option. In this way only the Serving MAAR is allowed to de-register the mobility session, arguing that the MN left definitely the domain.

Previous MAARs can, upon BCE expiry, send de-registration messages to the CMD, which, instead of acknowledging the message with a 0 lifetime, send back a PBA with a non-zero lifetime, hence renewing the session, if the MN is still connected to the domain.

The evaluation of these methods is left for future work.

3.6. Message Format

This section defines two Mobility Options to be used in the PBU and PBA messages:

   Previous MAAR Option;
   Serving MAAR Option.

In the current draft the messages reflect IPv6 format only. IPv4 compatibility will be added in next release.

3.6.1. Previous MAAR Option

This new option is defined for use with the Proxy Binding Acknowledgement messages exchanged by the CMD to a MAAR. This option is used to notify the S-MAAR about the previous MAAR’s global address and the prefix anchored to it. There can be multiple Previous MAAR options present in the message. Its format is as follows:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |     Length    | Prefix Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
```

P-MAAR’s address

3.6.2. Serving MAAR Option

This new option is defined for use with the Proxy Binding Update and Proxy Binding Acknowledgement messages exchanged between the CMD and a Previous MAAR. This option is used to notify the P-MAAR about the current Serving MAAR’s global address. Its format is as follows:

```
0                   1                   2                   3
+-------+-------+-------+-------+-------+-------+-------+-------+
|       |       |       |       |       |       |       |       |
+-------+-------+-------+-------+-------+-------+-------+-------+
|       |       |       |       |       |       |       |       |
+-------+-------+-------+-------+-------+-------+-------+-------+
```

| Type | Length |
|-------+--------|
|       |         |
|       |         |
|       +--------|
|       | S-MAAR’s address |

Type

To be assigned by IANA.

Length

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields. This field MUST be set to 34.

Prefix Length

8-bit unsigned integer indicating the prefix length of the IPv6 prefix contained in the option.

Previous MAAR’s address

A sixteen-byte field containing the P-MAAR’s IPv6 global address.

Home Network Prefix

A sixteen-byte field containing the mobile node’s IPv6 Home Network Prefix.
Type

To be assigned by IANA.

Length

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields. This field MUST be set to 16.

Serving MAAR’s address

A sixteen-byte field containing the S-MAAR’s IPv6 global address.

4. Fully distributed solution

In this section we introduce the guidelines to evolve our partially DMM solution into a fully distributed one. We list the key concepts in the following (some of the points are already enforced in previous sections of this document):

- All MAARs have a pool of global routable IPv6 prefixes to be assigned to MNs on the access link.
- Any central control entity is removed from the architecture and each MAAR will retain its own cache for the mobile nodes directly anchored to it.
- Both control and data planes are now entirely handled by the MAARs.

Because we aim for a fully distributed approach, the lack of knowledge of other MAARs and their advertised prefixes becomes a serious obstacle. In this particular case, when a MN attaches to a MAAR, there are two main pieces of information that this MAAR requires to know, to properly assure a mobile node’s mobility and continuity of its data flows: i) if the node has any P-MAARs and their addresses; ii) if it has P-MAARs, which prefixes were advertised by which MAAR.

There are several methods to achieve this:
Internet-Draft          A DMM solution for PMIPv6              July 2013

o Make before approaches, employing Layer 2 or Layer 3 mechanisms. The target MAAR is known in advance by the current MAAR before handover, hence the mobility context can be transferred.

o Distributed schemes for MAAR discovery: it can based on a peer-to-peer approach; or it can employ a unicast, multicast or broadcast query system.

o Explicit notification by the MN. For example, extending the layer three IP address configuration mechanisms (e.g., ND).

5. IANA Considerations

TBD.

6. Security Considerations

The solution assumes that the nodes are trusted and secure MAAR-to-MAAR communications are in place, for instance re-using the security mechanisms defined for PMIPv6. Thus, the solution does not introduce any new security vulnerability.

7. Acknowledgments

The authors would like to thank Marco Liebsch for his comments and discussion on this document.

8. References

8.1. Normative References


8.2. Informative References

In this section we describe how our solution addresses the DMM requirements listed in [I-D.ietf-dmm-requirements].

A.1. Distributed Processing

"IP mobility, network access and routing solutions provided by DMM MUST enable distributed processing for mobility management of some flows so that traffic does not need to traverse centrally deployed mobility anchors and thereby avoid non-optimal routes."

In our solution, a MAAR is responsible to handle the mobility for those IP flows started when the MN is attached to it. As long as the MN remains connected to the MAAR’s access links, the IP packets of such flows can benefit from the optimal path. When the MN moves to another MAAR, the path becomes non-optimal for ongoing flows, as they are anchored to the previous MAAR, but newly started IP sessions are forwarded by the new MAAR through the optimal path.

A.2. Transparency to Upper Layers when needed

"DMM solutions MUST provide transparent mobility support above the IP layer when needed. Such transparency is needed, for example, when, upon change of point of attachment to the network, an application flow cannot cope with a change in the IP address. However, it is not always necessary to maintain a stable home IP address or prefix for every application or at all times for a mobile node."
Our DMM solution operates at the IP layer, hence upper layers are totally transparent to the mobility operations. In particular, ongoing IP sessions are not disrupted after a change of access network. The routability of the old address is ensured by the IP tunnel with the old MAAR. New IP sessions are started with the new address. From the application’s perspective, those processes which sockets are bound to a unique IP address do not suffer any impact. For the other applications, the sockets bound to the old address are preserved, whereas next sockets use the new address.

A.3. IPv6 deployment

"DMM solutions SHOULD target IPv6 as the primary deployment environment and SHOULD NOT be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used."

The DMM solution we propose targets IPv6 only.

A.4. Existing mobility protocols

"A DMM solution SHOULD first consider reusing and extending IETF-standardized protocols before specifying new protocols."

This DMM solution is derived from the operations and messages specified in [RFC5213].

A.5. Co-existence with deployed networks and hosts

"The DMM solution MUST be able to co-exist with existing network deployments and end hosts. For example, depending on the environment in which DMM is deployed, DMM solutions may need to be compatible with other deployed mobility protocols or may need to co-exist with a network or mobile hosts/routers that do not support DMM protocols. The mobile node may also move between different access networks, where some of them may support neither DMM nor another mobility protocol. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when allowed by the trust relationship between them."
The partially DMM solution can be extended to provide a fallback mechanism to operate as legacy Proxy Mobile IPv6. It is necessary to instruct MAARs to always establish a tunnel with the same MAAR, working as LMA. The fully DMM solution can be extended as well, but it requires more intervention. The partially DMM solution can be deployed across different domains with trust agreements if the CMDs or the operators are enabled to transfer context from one node to another. The fully DMM solution works across multiple domains if both solution apply the same signalling scheme.

A.6. Security considerations

"DMM protocol solutions MUST consider security risks introduced by DMM into the network. Such considerations may include authentication and authorization mechanisms that allow a mobile host/router to use the mobility support provided by the DMM solution; measures against redirecting traffic to the wrong host when providing DMM support; signaling message protection for authentication, integrity and confidentiality."

The proposed solution does not specify a security mechanism, given that the same mechanism for PMIPv6 can be used.

A.7. Multicast

"DMM SHOULD enable multicast solutions in flexible distribution scenario. This flexibility pertains to the preservation of IP multicast nature from the perspective of a mobility entity and transmission of multicast packets to/from various multicast-enabled entities. Therefore, this flexibility enables different IP multicast flows with respect to a mobile host to be managed (e.g., subscribed, received and/or transmitted) using multiple multicast-enabled endpoints."

This solution in its current version does not specify any support for multicast traffic, which is left for study in future versions.

Appendix B. Implementation experience

The solution described in section Section 3.4 has been implemented in a real test-bed comprising 3 MAARs, one CMD, one MN and a CN. The CN is connected to the DMM domain through a router, which simulates the gateway to the internet cloud. All the machines used are Linux UBUNTU 10.04 systems with kernel 2.26.32, but the system has been tested also under newer platforms.

The code is developed in ANSI C from the existing UMIP implementation for PMIP within the framework of the MEDIEVAL EU project. The most
relevant changes with respect to the original version are related to
how to create the CMD and MAAR’s state machines from those of an LMA
and a MAG; for this purpose, part of the LMA code was copied to the
MAG, in order to send PBA messages and parse PBU. Also, the LMA
routing functions were removed completely, and moved to the MAG,
because MAARs need to route through the tunnels in downlink (as an
LMA) and in uplink (as a MAG).

Tunnel management is hence a relevant technical aspect, as multiple
tunnels are established by a single MAAR, which keeps their status
directly into the MN’s BCE. Indeed, from the implementation
experience it was chosen to create an ancillary data structure as
field within a BCE: the data structure is called "MAAR list" and
stores the previous MAARs’ address and the corresponding prefix(es)
assigned for the MN. Only the CMD and the serving MAAR store this
data structure, because the CMD maintains the global MN’s mobility
session formed during the MN’s roaming within the domain, and the
serving MAAR needs to know which previous MAARs were visited, the
prefix(es) they assigned and the tunnels established with them.
Conversely, a previous MAAR only needs to know which is the current
Serving MAAR and establish a single tunnel with it. For this reason,
a MAAR that receives a PBU from the CMD (meaning that the MN attached
to another MAAR), first sets up the routing state for the MN’s
prefix(es) it is anchoring, then stop the BCE expiry timer and
deletes the MAAR list (if present) since it is no longer useful.

In order to have the MN totally unaware of the changes in the access
link, all MAARs exhibit the same L2 and L3 identifiers in the access
interface (as the PMIPv6 Fixed MAG Link Local Address feature). A
solution is under study to avoid this configuration and influence the
MN on the source address choice. Moreover, it should be noted that
the protocols designed in the document work only at the network layer
to handle the MNs joining or leaving the domain. This should
 guarantee a certain independency to a particular access technology.
The implementation reflects this reasoning, but we argue that an
interaction with lower layers produces a more effective attachment
and detachment detection, therefore improving the performance, also
regarding de-registration mechanisms.

It was chosen to implement the "proxy" solution because it produces
the shortest handover latency, but a slight modification on the CMD
state machine can produce the first scenario described ("relay")
which guarantees a more consistent request/ack scheme between the
MAARs. By modifying also the MAAR’s state machine it can be
implemented the second solution ("locator").

A prototype implementation of the solution described in this
document, together with the distributed logical interface concept
specified in [I-D.bernardos-dmm-distributed-anchoring] was shown during IETF 83rd, in Paris in March 2012. An enhancement version of this demo is going to be presented at the 87th IETF meeting in Berlin, July 2013. The new demo includes a use case scenario employing a CDN system for video delivery.

Authors’ Addresses

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain  
Phone: +34 91624 6236  
Email: cjbc@it.uc3m.es  
URI: http://www.it.uc3m.es/cjbc/

Antonio de la Oliva  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain  
Phone: +34 91624 8803  
Email: aoliva@it.uc3m.es  
URI: http://www.it.uc3m.es/aoliva/

Fabio Giust  
Institute IMDEA Networks and Universidad Carlos III de Madrid  
Av. del Mar Mediterraneo, 22  
Leganes, Madrid 28918  
Spain  
Phone: +34 91481 6979  
Email: fabio.giust@imdea.org
Abstract

This document introduces a framework for mobility management protocols in terms of their key, abstract logical functions. We explain how the framework is capable of presenting a unified view, reducing the clutter that prevents a casual reader from understanding the commonalities between different approaches in mobility management. A first order application of this framework is to enable us to examine previously standardized mobility management protocols, such as MIPv6 and PMIPv6 (as well as several of their extensions), and describe their core functionality in terms of different configurations of the logical functions defined by the framework.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 29, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Table of Contents

1. Introduction ................................................. 3
2. Conventions and Terminology ................................. 4
3. Mobility Management Logical Functions ..................... 4
   4.1. Decomposing Mobile IPv6 .............................. 6
   4.2. From MIPv6 to PMIPv6 .................................. 6
   4.3. Hierarchical Mobile IPv6 .............................. 8
   4.4. Distributing Mobility Anchors ......................... 9
   4.5. Migrating Home Agents ................................ 10
5. DMM Functional Decomposition Scenarios ..................... 11
   5.1. Flat Network Scenario ................................ 11
      5.1.1. Network-based Mobility Management ................ 12
      5.1.2. Client-based Mobility Management ................. 13
   5.2. DMM with Control and Data Plane Separation ............ 14
6. Security Considerations .................................... 16
7. IANA Considerations ........................................ 16
8. References ................................................. 16
   8.1. Normative References .................................. 16
   8.2. Informative References ................................. 16
Authors’ Addresses .............................................. 18
1. Introduction

While there is ongoing research on new protocols for distributed mobility management (DMM), it has also been proposed, e.g., in [Paper-Distributed.Mobility.PMIP] and in other publications, that a DMM architecture can be designed using primarily existing mobility management protocols with some extensions. This is reflected in the requirement included in [I-D.ietf-dmm-requirements]: distributed mobility management is to first use existing protocols and their extensions before considering new protocol designs. Although this a key requirement as we move forward, it does not point to which extensions are needed let alone how to devise them.

Mobile IPv6 [RFC6275], for instance, which is a logically centralized mobility management approach addressing primarily hierarchical mobile networks, has numerous variants and extensions including, PMIPv6 [RFC5213], Hierarchical MIPv6 (HMIPv6) [RFC5380], Fast MIPv6 (FMIPv6) [RFC5568] [RFC4988], Proxy-based FMIPv6 (PFMIPv6) [RFC5949], just to name a few. These variants or extensions of MIPv6 have been developed over the years owing to the different needs that have been arising ever since the first MIP specification came into life. This document argues that we can gain much more insight into the design space of DMM protocols by abstracting the functionality of existing mobility management protocols in terms of logical functions. Different variants of existing mobility management protocols can then be expressed as different design variations of how these logical functions are put together. The result is a rich framework that can express sophisticated functionalities in a more straightforward manner. What is more, this document shows how to reconfigure these logical functions towards various distributed mobility management designs.

The rest of this document is organized as follows. After setting the stage with conventions and terminology in the following section, Section 3 introduces the framework abstractions, based on common functionality we observe in the current crop of mobility management protocols. This includes three logical functions, namely, home address allocation, mobility routing and location management. Such functional decomposition will enable us to clearly separate data and control plane functionality, and gives us the flexibility in an implementation to position said logical functions at their most appropriate places in the system design. Next, Section 4 shows that these logical functions can indeed perform the same functions as major existing mobility protocols. These functions therefore become the foundation for a unified framework upon which different designs of distributed mobility management may be built upon. Finally, Section 5 presents scenarios where the functional aspects of the framework are illustrated.
2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275] and in the Proxy Mobile IPv6 specification [RFC5213]. This includes terms such as mobile node (MN), correspondent node (CN), home agent (HA), home address (HoA), care-of-address (CoA), local mobility anchor (LMA), and mobile access gateway (MAG).

In addition, this document uses the following term:

Home network of an application session (or of an HoA) is the network that has allocated the IP address (HoA) used for the session identifier by the application running in an MN. The MN may be attached to more than one home networks.

3. Mobility Management Logical Functions

Functional entity (FE) decomposition is an often-used engineering approach that enables us to look at the similarities and differences of complex systems while keeping track of their important operational aspects. Earlier work, for instance, in the European research project Ambient Networks investigated how to create an advanced and forward-looking architecture aiming primarily for mobile and wireless networks [Book-AN]. A key goal was to design mechanisms that can be deployed in a variety of settings (ad-hoc or operator-controlled) and scale from small home networks with little human supervision to sensor networks deployed over large geographical areas with limited resources, to large professionally-managed infrastructure networks. The project put forward the concept of the Ambient Control Space (ACS) which relies on only three interfaces; interested readers can find more details in [Book-AN].

Within the ACS, novel mobility management mechanisms were developed based on the concept of self-containing Functional Entities (FEs) which featured well-defined interfaces and interactions with each other. This systematic decomposition enabled the development of several mobility management mechanisms which put emphasis on different aspects. Examples of these approaches include the Generic Link Layer [Paper-GLL], Multi-radio Resource Management [Paper-MRRM], and [Paper-NODEID], which has some similarities with HIP. Later work in this area capitalized on the established FEs within the ACS to
define new mechanisms, that were not originally envisioned, such as [Paper-ANHASA].

Following this tradition, this document applies a similar approach to logically decomposing mobility management functions. This way we can establish a common framework that will enable us to reason about DMM functionality with well-defined and well-understood FEs or logical functions. As a first step, the DMM Framework presented in this document demonstrates that the existing mobility management functions of MIPv6, PMIPv6, and HMIPv6 can be abstracted into the following logical functions:

1. Anchoring function: allocation of home network prefix or HoA to an MN that registers with the network;

2. Mobility Router (MR) function: packets interception and forwarding to/from the MN HoA based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination;

3. Internetwork Location Management (LM) function: managing and keeping track of the MN internetwork location, which includes a mapping of the HoA to the mobility anchoring point that the MN is anchored to;

4. Location Update (LU) function: provisioning of MN location information to the LM function;

5. Routing Control (RC) function: MR function forwarding state configuration.

In addition, the Access Router (AR) logical function provides first-hop network access and includes functionality below the network layer, e.g. radio communication facilities. An AR may provide home address allocation as well as act as MR.

4. Mobility Protocol Functional Decomposition

This section shows that existing mobility management protocols can be expressed as different configurations of the logical functions introduced in Section 3 above. Using these generic logical functions, we will build up the existing mobility protocols one step at a time in the following sequence: MIPv6, PMIPv6, HMIPv6, and HAHA. Functions are added and modified as needed in each step.
4.1. Decomposing Mobile IPv6

Fig. 1 illustrates the Mobile IPv6 [RFC6275] functional decomposition using the logical functions introduced in Section 3. The combination of the MR, LM and HoA allocation logical functions in Network1 effectively defines the home agent or the mobility anchor. In the depicted network scenario, the mobile node designated as MN11 was originally attached to Network1 and was allocated an IP prefix for its home address (HoA11). At a later stage, MN11 moves to Network3, where it is allocated a new prefix to configure the IP address IP32. LM1 maintains the binding HoA11:IP32 so that packets from its correspondent node CN21 in Network2 destined to HoA11 can be intercepted by MR1, which will then tunnel them to IP32. MN11 must perform mobility signaling using the LU function.

```
+-----+ +-----+ +-----+
|     |   |     |
| LM1 |   |     |
+-----+   +-----+

location=IP32

HoA1 alc  IP3 alc  IP2 alc

+-----+ +-----+ +-----+
|     |   |     |
| MR1 |   |     |
+-----+   +-----+

MN31  MN11  +LU  CN21

HoA11  IP31  IP32,  HoA11
```

Figure 1. Functional decomposition of Mobile IPv6

4.2. From MIPv6 to PMIPv6

The functional decomposition of Proxy Mobile IPv6 [RFC5213] according to the proposed framework is shown in Fig. 2. In PMIPv6, the combination of LM, MR, and HoA allocation effectively defines the Local Mobility Anchor (LMA). The combination of AR and LU together with additional signaling with MN comprises the Mobile Access Gateway (MAG). In the figure, MN11 is attached to the access router AR31 which has the IP address IP31 in Network3. LM1 maintains the binding HoA11:IP31. The access router AR31 also behaves like a home link to MN11 so that MN11 can use its original IP address HoA11.
MIPv6 and PMIPv6 both employ the same concept of separating the session identifier (HoA) from the routing address (CoA). Fig. 3 contrasts (a) MIPv6 with (b) PMIPv6 by illustrating the destination IP address in the network-layer header as a packet traverses the network from the CN to the MN. Note that MIPv6 and PMIPv6 bundle three mobility management logical functions, namely, LM1, IP1 prefix allocation and MR1 into the home agent (HA) and Local Mobility Anchor (LMA), respectively.

Fig. 3 shows that, as far as data-plane traffic is concerned, routing from CN to MN+LU in MIPv6 is similar to the route from CN to AR+LU in PMIPv6. The difference is in that in the former case, the MN with the LU function is substituted by the combination of the AR with the LU function and the MN. While additional signaling is needed to enable the combination of AR+LU and MN to behave like MN+LU in MIPv6, such signaling can be confined between the AR+LU and the MN only. It can therefore be seen under this unified formulation, that a host-based mobility management protocol can be translated using this substitution into a network-based mobility management protocol and vice versa.
Figure 3. Network layer in the protocol stack of packets sent from the CN and tunneled (a) to the MN+LU in MIPv6; and (b) to the AR+LU in PMIPv6 showing the destination IP address as the packet traverses from the CN to the MN.

4.3. Hierarchical Mobile IPv6

The functional decomposition of Hierarchical Mobile IPv6 [RFC5380] is shown in Fig. 4. Besides the logical functions LM1, MR1, and HoA1 prefix allocation in Network1, as we have seen above for MIPv6 and PMIPv6, there is an MR function (MR3) in the visited network (Network3). MR3 acts also as a proxy between LM1 and MN11 in the hierarchical LM function LM1--MR3--MN11. That is, LM1 maintains the LM binding HoA11:MR3 while MR3 tracks the LM binding HoA11:IP32. The combined function of MR and the LM proxy function is the Mobility Anchor Point (MAP).
Figure 4. Functional decomposition of Hierarchical Mobile IPv6

Note that as depicted in Fig. 4, if MN11 takes the place of MN31 which is attached to AR31, the resulting mobility management becomes network-based.

4.4. Distributing Mobility Anchors

As we have seen so far, the framework is sufficiently expressive to enable us to decompose the major MIPv6 variants. It is possible to replicate the mobility anchoring function for any of MIPv6, PMIPv6, or HMIPv6, in multiple networks as shown in Fig. 5 which illustrates such an example with three networks.
4.5. Migrating Home Agents

When all logical functions of the Framework are bundled into a single entity e.g., a home agent in MIPv6 or a local mobility anchor in PMIPv6, in a single network, the result is triangular routing when the MN and the CN are in networks close to each other but are far from the anchor point. A method to solve the triangle routing problem is to duplicate the anchor points in many networks in different geographic locations as advocated in [Paper-Migrating.Home.Agents]. A functional decomposition of Migrating Home Agents is shown in Fig. 6: the MR function is available in each of the three networks Network1, Network2, and Network3. The LM function in each network (LM0) contains the LM information for all three networks. Each MR in each network advertises the HoA IP prefixes of all these networks using anycast. Traffic from CN21 in Network2 destined to HoA11 will therefore be intercepted by the MR nearest to the CN, i.e. MR2 in the example of Fig. 6. Using the LM information in LM0, MR2 will use the binding HoA11:IP32 to tunnel the packets to MN11.
Similarly, traffic originating from MN11 will be served by its nearest MR (MR3). Triangular routing is therefore avoided. Yet the synchronization of all home agents becomes a challenge as discussed in [Paper-SMGI]. In addition, the amount of signaling traffic necessary for synchronizing the home agents may become excessive when both the number of mobile nodes and the number of home agents increase.

As before, if MN11 in Fig. 6 takes the place of MN31 which is attached to AR31, the resulting mobility management becomes network-based.

5. DMM Functional Decomposition Scenarios

This section covers the functional description of DMM. Basically, the scenarios present a way to distribute the logical mobility functions.

5.1. Flat Network Scenario

In a flat network, the logical functions may all be located at the AR as shown in Figs. 7 and 8, respectively. For example,
[I-D.seite-dmm-dma] and [I-D.bernardos-dmm-distributed-anchoring] are PMIPv6-based implementations of this scenario. These two figures depict the network- and client-based distributed mobility management scenarios, respectively. AR is expected to support the HoA allocation function. Then, depending on the mobility situation of the MN, the AR can run different functions:

1. AR can act as a standard IP router;
2. AR can provide the MR function (i.e. act as mobility anchor);
3. AR can provide the LU function;
4. AR can provide both MR and LU functions.

5.1.1. Network-based Mobility Management

The functional decomposition of network-based mobility management is depicted in Fig. 7. In case (1), MN1 attaches to AR1. AR advertises the prefix HoA1 to MN1 and then acts as a legacy IP router. MN1 initiates a communication with CN11.

In case (2), MN1 performs a handover from AR1 to AR3 while maintaining ongoing IP communication with CN11. AR1 becomes the mobility anchor for the MN1-CN11 IP communication: AR1 runs MR and LM functions on behalf of MN1. AR3 performs LU up to the LM in AR1: AR3 indicates to AR1 the new location of the MN1. AR3 allocates a new IP prefix (HoA3) for new IP communications. That is, HoA3 is used for all new IP communications, e.g., if MN1 initiates IP communication with CN21. AR3 shall act as a legacy IP router for MN1-CN21 communication.

In case (3), MN1 performs a handover from AR1 to AR2 with ongoing IP communication with CN11 and CN21. AR1 is the mobility anchor for the MN1-CN11 IP communication. AR3 becomes the mobility anchor for the MN1-CN21 IP communication. Both AR1 and AR3 run MR and LM functions for MN1, respectively, anchoring HoA1 and HoA3. AR2 performs location updates up to the LMs in AR1 and AR3 for respectively relocate HoA1 and HoA3.
5.1.2. Client-based Mobility Management

The functional decomposition of client-based mobility management is depicted in Fig. 8. In case (1), MN1 attaches to AR1. AR advertises the prefix HoA1 to MN1 and then acts as a legacy IP router. MN1 initiates a communication with CN11.

In case (2), MN1 performs a handover from AR1 to AR3 while maintaining ongoing IP communication with CN11. AR1 becomes the mobility anchor for the MN1-CN11 IP communication: AR1 runs MR and LM functions for MN1. The MN performs LU directly up to the LM in AR1.
or via AR3; in this case AR3 acts as a proxy locator (pLU) (e.g. as a FA in MIPv4). AR3 allocates a new IP prefix (HoA3) for new IP communications. HoA3 is supposed to be used for new IP communications, e.g., if MN1 initiates IP communication with CN21. AR3 shall act as a legacy IP router for MN1-CN21 communication.

5.2. DMM with Control and Data Plane Separation

This section considers a scenario which involves multiple MRs and a distributed LM database. The different use case scenarios of distributed mobility management are described in [I-D.yokota-dmm-scenario] as well as in [Paper-Distributed.Mobility.Review]. The functional decomposition described in this document can be used to understand better the data and control plane separation.

Fig. 9 shows an example DMM topology with the same three networks we have been using in Fig. 5. As in Fig. 5, each network in Fig. 9 has its own IP prefix allocation function. In the data plane, the mobility routing function is distributed to multiple locations at the MRs so that routing can be optimized. In the control plane, the MRs may exchange information with each other.

In addition to these features, the LM function in Fig. 9 is a distributed database, possibly implemented with multiple virtual or physical servers, handling the mapping of HoA to CoA. To perform
mobility routing, the MRs need the location information which is maintained at LM1, LM2, and LM3. The MRs are, therefore, the clients of the LM servers and may also send location updates to the LM as the MNs perform the handover. The location information may either be pulled from the LM servers by the MR, or pushed to the MR by the LM servers. In addition, the MR may also cache a limited amount of location information.

Fig. 9 illustrates three MRs (MR1, MR2, and MR3) in three networks. In this scenario we take that MN11 has moved from Network1 supported by MR1 and LM1 to Network3 supported by MR3 and LM3. MN11 may use the homa address (HoA11) allocated to it when it was directly connected to the former network for those application sessions that...
were started when the mobile node was attached there and do require session continuity after the handover to the latter network. When MN11 is connected to Network1, no location management is needed; LM1 will not keep an entry for HoA11. After MN11 handovers to Network3, the LM1 server maintains a mapping of HoA11 to MR3. That is, LM1 points to Network3 and it is this network that will keep track of how to reach MN11. Such a hierarchical mapping can prevent frequent signaling updates to LM1, as MN11 performs intra-network handover(s) within the Network3 domain. In other words, the concept of hierarchical mobile IP [RFC5380] is applied here for location management only but not for data plane routing.

6. Security Considerations

TBD

7. IANA Considerations

This document presents no IANA considerations.

8. References

8.1. Normative References


8.2. Informative References


[I-D.ietf-dmm-requirements] Chan (Ed.) et al., H., "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-03 (work in progress), December 2012.

[I-D.seite-dmm-dma] Seite, P., Bertin, P., and JH. Lee, "Distributed Mobility
Anchoring”, draft-seite-dmm-dma-06 (work in progress), January 2013.

[I-D.yokota-dmm-scenario]
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

[Paper-ANHASA]

[Paper-Distributed.Mobility.PMIP]

[Paper-Distributed.Mobility.Review]

[Paper-GLL]

[Paper-MRRM]


Authors' Addresses

H Anthony Chan
Huawei Technologies
5340 Legacy Dr. Building 3
Plano, TX 75024
USA

Email: h.a.chan@ieee.org
Pierrick Seite
France Telecom - Orange
4, rue du Clos Courtel, BP 91226
Cesson-Sevigne 35512
France

Email: pierrick.seite@orange-ftgroup.com

Kostas Pentikousis
Huawei Technologies
Carnotstrasse 4
10587 Berlin
Germany

Email: k.pentikousis@huawei.com
Abstract

This document analyzes deployment practices of existing IP mobility protocols in a distributed mobility management environment. It then identifies existing limitations when compared to the requirements defined for a distributed mobility management solution.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 8, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of
1. Introduction

Existing network-layer mobility management protocols have primarily employed a mobility anchor to ensure connectivity of a mobile node by forwarding packets destined to, or sent from, the mobile node after the node has moved to a different network. The mobility anchor has been centrally deployed in the sense that the traffic of millions of mobile nodes in an operator network is typically managed by the same anchor. This centralized deployment of mobility anchors to manage IP sessions poses several problems. In order to address these problems, a distributed mobility management (DMM) architecture has been
This document investigates whether it is feasible to deploy current IP mobility protocols in a DMM scenario in a way that can fulfill the requirements as defined in [RFC7333]. It discusses current deployment practices of existing mobility protocols and identifies the limitations (gaps) in these practices from the standpoint of satisfying DMM requirements. The analysis is primarily towards IPv6 deployment, but can be seen to also apply to IPv4 whenever there are IPv4 counterparts equivalent to the IPv6 mobility protocols.

The rest of this document is organized as follows. Section 3 analyzes existing IP mobility protocols by examining their functions and how these functions can be configured and used to work in a DMM environment. Section 4 presents the current practices of IP wireless networks and 3GPP architectures. Both network- and host-based mobility protocols are considered. Section 5 presents the gap analysis with respect to the current practices.

2. Terminology

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], in the Proxy Mobile IPv6 specification [RFC5213], and in the Distributed Mobility Management Requirements [RFC7333]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), Local Mobility Anchor (LMA), Mobile Access Gateway (MAG), centrally deployed mobility anchors, distributed mobility management, hierarchical mobile network, flatter mobile network, and flattening mobile network.

In addition, this document also introduces some definitions of IP mobility functions in Section 3.

In this document there are also references to a "distributed mobility management environment." By this term, we refer to a scenario in which the IP mobility, access network and routing solutions allow for setting up IP networks so that traffic is distributed in an optimal way, without relying on centrally deployed mobility anchors to manage IP mobility sessions.

3. Functions of existing mobility protocols

The host-based Mobile IPv6 (MIPv6) [RFC6275] and its network-based extension, Proxy Mobile IPv6 (PMIPv6) [RFC5213], as well as Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] are logically centralized mobility management approaches addressing primarily hierarchical mobile networks. Although these approaches are centralized, they have important mobility management functions resulting from years of
extensive work to develop and to extend these functions. It is therefore useful to take these existing functions and examine them in a DMM scenario in order to understand how to deploy the existing mobility protocols to provide distributed mobility management.

The main mobility management functions of MIPv6, PMIPv6, and HMIPv6 are the following:

1. Anchoring Function (AF): allocation to a mobile node of an IP address, i.e., Home Address (HoA), or prefix, i.e., Home Network Prefix (HNP) topologically anchored by the advertising node. That is, the anchor node is able to advertise a connected route into the routing infrastructure for the allocated IP prefixes. This function is a control plane function.

2. Internetwork Location Information (LI) function: managing and keeping track of the internetwork location of an MN. The location information may be a binding of the IP advertised address/prefix, e.g., HoA or HNP, to the IP routing address of the MN or of a node that can forward packets destined to the MN. It is a control plane function.

   In a client-server protocol model, location query and update messages may be exchanged between a location information client (LIc) and a location information server (LIs).

3. Forwarding Management (FM) function: packet interception and forwarding to/from the IP address/prefix assigned to the MN, based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination.

   FM may optionally be split into the control plane (FM-CP) and data plane (FM-DP).

In Mobile IPv6, the home agent (HA) typically provides the anchoring function (AF); the location information server (LIs) is at the HA whereas the location information client (LIc) is at the MN; the Forwarding Management (FM) function is distributed between the ends of the tunnel at the HA and the MN.

In Proxy Mobile IPv6, the Local Mobility Anchor (LMA) provides the anchoring function (AF); the location information server (LIs) is at the LMA whereas the location information client (LIc) is at the mobile access gateway (MAG); the Forwarding Management (FM) function is distributed between the ends of the tunnel at the HA and the MAG.
In Hierarchical Mobile IPv6 (HMIPv6) [RFC5380], the Mobility Anchor Point (MAP) serves as a location information aggregator between the LIs at the HA and the LIc at the MN. The MAP also provides the FM function to enable tunneling between HA and itself as well as tunneling between MN and itself.

4. DMM practices

This section documents deployment practices of existing mobility protocols to satisfy distributed mobility management requirements. This description considers both IP wireless, e.g., evolved Wi-Fi hotspots, and 3GPP flattening mobile network.

While describing the current DMM practices, the section provides references to the generic mobility management functions described in Section 3 as well as some initial hints on the identified gaps with respect to the DMM requirements documented in [RFC7333].

4.1. Assumptions

There are many different approaches that can be considered to implement and deploy a distributed anchoring and mobility solution. The focus of the gap analysis is on certain current mobile network architectures and standardized IP mobility solutions, considering any kind of deployment options which do not violate the original protocol specifications. In order to limit the scope of our analysis of DMM practices, we consider the following list of technical assumptions:

1. Both host- and network-based solutions are considered.
2. Solutions should allow selecting and using the most appropriate IP anchor among a set of available candidates.
3. Mobility management should be realized by the preservation of the IP address across the different points of attachment (i.e., provision of IP address continuity). This is in contrast to certain transport-layer based approaches such as Stream Control Transmission Protocol (SCTP) [RFC4960] or application-layer mobility.

Applications which can cope with changes in the MN’s IP address do not depend on IP mobility management protocols such as DMM. Typically, a connection manager together with the operating system will configure the source address selection mechanism of the IP stack. This might involve identifying application capabilities and triggering the mobility support accordingly. Further considerations on application management and source address selection are out of the scope of this document, but the reader might consult [RFC6724].
4.2. IP flat wireless network

This section focuses on common IP wireless network architectures and how they can be flattened from an IP mobility and anchoring point of view using common and standardized protocols. We take Wi-Fi as an useful wireless technology, since it is widely known and deployed nowadays. Some representative examples of Wi-Fi deployment architectures are depicted in Figure 1.

In Figure 1, three typical deployment options are shown [I-D.gundavelli-v6ops-community-wifi-svcs]. On the left hand side of the figure, mobile nodes MN1 and MN2 directly connect to a Residential Gateway (RG) at the customer premises. The RG hosts the 802.11 Access Point (AP) function to enable wireless layer-2 access connectivity and also provides layer-3 routing functions. In the middle of the figure, mobile nodes MN3 and MN4 connect to Wi-Fi Access Points (APs) AP1 and AP2 that are managed by a Wireless LAN Controller (WLC), which performs radio resource management on the APs, domain-wide mobility policy enforcement and centralized forwarding function for the user traffic. The WLC could also implement layer-3 routing functions, or attach to an access router (AR). Last, on the right-hand side of the figure, access points AP3
and AP4 are directly connected to an access router. This can also be used as a generic connectivity model.

IP mobility protocols can be used to provide heterogeneous network mobility support to users, e.g., handover from Wi-Fi to cellular access. Two kinds of protocols can be used: Proxy Mobile IPv6 [RFC5213] or Mobile IPv6 [RFC5555], with the role of mobility anchor, e.g., Local Mobility Anchor or home agent, typically being played by the edge router of the mobile network [SDO-3GPP.23.402].

Although this section has made use of the example of Wi-Fi networks, there are other flattening mobile network architectures specified, such as WiMAX [IEEE.802-16.2009], which integrates both host- and network-based IP mobility functions.

Existing IP mobility protocols can also be deployed in a flatter manner, so that the anchoring and access aggregation functions are distributed. We next describe several practices for the deployment of existing mobility protocols in a distributed mobility management environment. The analysis in this section is limited to protocol solutions based on existing IP mobility protocols, either host- or network-based, such as Mobile IPv6 [RFC6275], [RFC5555], Proxy Mobile IPv6 (PMIPv6) [RFC5213], [RFC5844] and Network Mobility Basic Support protocol (NEMO) [RFC3963]. Extensions to these base protocol solutions are also considered. The analysis is divided into two parts: host- and network-based practices.

4.2.1. Host-based IP DMM practices

Mobile IPv6 (MIPv6) [RFC6275] and its extension to support mobile networks, the NEMO Basic Support protocol (hereafter, simply referred to as NEMO) [RFC3963] are well-known host-based IP mobility protocols. They depend on the function of the Home Agent (HA), a centralized anchor, to provide mobile nodes (hosts and routers) with mobility support. In these approaches, the Home Agent typically provides the Anchoring Function (AF), Forwarding Management (FM), and Internetwork Location Information server (LIs) functions. The mobile node possesses the Location Information client (Lic) function and the FM function to enable tunneling between HA and itself. We next describe some practices that show how MIPv6/NEMO and several other protocol extensions can be deployed in a distributed mobility management environment.

One approach to distribute the anchors can be to deploy several HAs (as shown in Figure 2), and assign the topologically closest anchor to each MN [RFC4640], [RFC5026], [RFC6611]. In the example shown in Figure 2, the mobile node MN1 is assigned to the home agent HA1 and uses a home address anchored by HA1 to communicate with the
correspondent node CN1. Similarly, the mobile node MN2 is assigned to the home agent HA2 and uses a home address anchored by HA2 to communicate with the correspondent node CN2. Note that MIPv6/NEMO specifications do not prevent the simultaneous use of multiple home agents by a single mobile node. In this deployment model, the mobile node can use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. However, there is currently no mechanism specified in IETF standard to enable an efficient dynamic discovery of available anchors and the selection of the most suitable one.

Figure 2: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

One goal of the deployment of mobility protocols in a distributed mobility management environment is to avoid the suboptimal routing caused by centralized anchoring. Here, the Route Optimization (RO) support provided by Mobile IPv6 can be used to achieve a flatter IP data forwarding. By default, Mobile IPv6 and NEMO use the so-called Bidirectional Tunnel (BT) mode, in which data traffic is always encapsulated between the MN and its HA before being directed to any other destination. The RO mode allows the MN to update its current location on the CNs, and then use the direct path between them. Using the example shown in Figure 2, MN1 is using BT mode with CN1,
while MN2 is in RO mode with CN2. However, the RO mode has several drawbacks:

- The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol because of the security problems posed by extending return routability tests for prefixes, although many different solutions have been proposed [RFC4889].

- The RO mode requires signaling that adds some protocol overhead.

- The signaling required to enable RO involves the home agent and is repeated periodically for security reasons [RFC4225]. Therefore the HA remains a single point of failure.

- The RO mode requires support from the CN.

Notwithstanding these considerations, the RO mode does offer the possibility of substantially reducing traffic through the Home Agent, in cases when it can be supported by the relevant correspondent nodes. Note that a mobile node can also use its care-of-address (CoA) directly [RFC5014] when communicating with CNs on the same link or anywhere in the Internet, although no session continuity support would be provided by the IP stack in this case.

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] (as shown in Figure 3), is another host-based IP mobility extension which can be considered as a complement to provide a less centralized mobility deployment. It allows the reduction of the amount of mobility signaling as well as improving the overall handover performance of Mobile IPv6 by introducing a new hierarchy level to handle local mobility. The Mobility Anchor Point (MAP) entity is introduced as a local mobility handling node deployed closer to the mobile node. It provides LI intermediary function between the LI server (LIs) at the HA and the LI client (LIC) at the MN. It also performs the FM function to tunnel with the HA and also with the MN.
When HMIPv6 is used, the MN has two different temporary addresses: the Regional Care-of Address (RCoA) and the Local Care-of Address (LCoA). The RCoA is anchored at one MAP, which plays the role of local home agent, while the LCoA is anchored at the access router level. The mobile node uses the RCoA as the CoA signaled to its home agent. Therefore, while roaming within a local domain handled by the same MAP, the mobile node does not need to update its home agent, i.e., the mobile node does not change its RCoA.

The use of HMIPv6 enables a form of route optimization, since a mobile node may decide to directly use the RCoA as source address for a communication with a given correspondent node, particularly if the MN does not expect to move outside the local domain during the lifetime of the communication. This can be seen as a potential DMM mode of operation, though it fails to provide session continuity if and when the MN moves outside the local domain. In the example shown in Figure 3, MN1 is using its global HoA to communicate with CN1, while it is using its RCoA to communicate with CN2.

Furthermore, a local domain might have several MAPs deployed, enabling therefore a different kind of HMIPv6 deployments which are
flattening and distributed. The HMIPv6 specification supports a flexible selection of the MAP, including those based on the distance between the MN and the MAP, or taking into consideration the expected mobility pattern of the MN.

Another extension that can be used to help with distributing mobility management functions is the Home Agent switch specification [RFC5142], which defines a new mobility header for signaling a mobile node that it should acquire a new home agent. [RFC5142] does not specify the case of changing the mobile node’s home address, as that might imply loss of connectivity for ongoing persistent connections. Nevertheless, that specification could be used to force the change of home agent in those situations where there are no active persistent data sessions that cannot cope with a change of home address.

There are other host-based approaches standardized that can be used to provide mobility support. For example MOBIKE [RFC4555] allows a mobile node encrypting traffic through IKEv2 [RFC5996] to change its point of attachment while maintaining a Virtual Private Network (VPN) session. The MOBIKE protocol allows updating the VPN Security Associations (SAs) in cases where the base connection initially used is lost and needs to be re-established. The use of the MOBIKE protocol avoids having to perform an IKEv2 re-negotiation. Similar considerations to those made for Mobile IPv6 can be applied to MOBIKE; though MOBIKE is best suited for situations where the address of at least one endpoint is relatively stable and can be discovered using existing mechanisms such as DNS.

Extensions have been defined to the mobility protocol to optimize the handover performance. Mobile IPv6 Fast Handovers (FMIPv6) [RFC5568] is the extension to optimize handover latency. It defines new access router discovery mechanism before handover to reduce the new network discovery latency. It also defines a tunnel between the previous access router and the new access router to reduce the packet loss during handover. The Candidate Access Router Discovery (CARD) [RFC4066] and Context Transfer Protocol (CXTP) [RFC4067] protocols were standardized to improve the handover performance. The DMM deployment practice discussed in this section can also use those extensions to improve the handover performance.

4.2.2. Network-based IP DMM practices

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is the main network-based IP mobility protocol specified for IPv6. Proxy Mobile IPv4 [RFC5844] defines some IPv4 extensions. With network-based IP mobility protocols, the Local Mobility Anchor (LMA) typically provides the Anchoring Function (AF), Forwarding Management (FM) function, and Internetwork Location Information server (LI) function. The mobile
access gateway (MAG) provides the Location Information client (LiC) function and Forwarding Management (FM) function to tunnel with LMA. PMIPv6 is architecturally almost identical to MIPv6, as the mobility signaling and routing between LMA and MAG in PMIPv6 is similar to those between HA and MN in MIPv6. The required mobility functionality at the MN is provided by the MAG so that the involvement in mobility support by the MN is not required.

We next describe some practices that show how network-based mobility protocols and several other protocol extensions can be deployed in a distributed mobility management environment.

One way to decentralize Proxy Mobile IPv6 operation can be to deploy several Local Mobility Anchors and use some selection criteria to assign LMAs to attaching mobile nodes. An example of this type of assignment is shown in Figure 4. As with the client based approach, a mobile node may use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. This assignment can be static or dynamic. The main advantage of this simple approach is that the IP address anchor, i.e., the LMA, could be placed closer to the mobile node. Therefore the resulting paths are close-to-optimal. On the other hand, as soon as the mobile node moves, the resulting path will start deviating from the optimal one.

![Figure 4: Distributed operation of Proxy Mobile IPv6](image)

In a similar way to the host-based IP mobility case, network-based IP mobility has some extensions defined to mitigate the suboptimal routing issues that may arise due to the use of a centralized anchor. The Local Routing extensions [RFC6705] enable optimal routing in Proxy Mobile IPv6 in three cases: i) when two communicating MNs are attached to the same MAG and LMA, ii) when two communicating MNs are attached to different MAGs but to the same LMA, and iii) when two communicating MNs are attached to the same MAG but have different LMAs. In these three cases, data traffic between the two mobile nodes does not traverse the LMA(s), thus providing some form of path optimization since the traffic is locally routed at the edge. The main disadvantage of this approach is that it only tackles the MN-to-MN communication scenario, and only under certain circumstances.

An interesting extension that can also be used to facilitate the deployment of network-based mobility protocols in a distributed mobility management environment is the support of LMA runtime assignment described in [RFC6463]. This extension specifies a runtime Local Mobility Anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime Local Mobility Anchor assignment takes place during the Proxy Binding Update / Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism is mainly aimed for load-balancing purposes, it can also be used to select an optimal LMA from the routing point of view. A runtime LMA assignment can be used to change the assigned LMA of an MN, for example, in cases when the mobile node does not have any active session, or when the running sessions can survive an IP address change. Note that several possible dynamic Local Mobility Anchor discovery solutions can be used, as described in [RFC6097].

4.3. Flattening 3GPP mobile network approaches

The 3rd Generation Partnership Project (3GPP) is the standards development organization that specifies the 3rd generation mobile network and the Evolved Packet System (EPS) [SDO-3GPP.23.402], which mainly comprises the Evolved Packet Core (EPC) and a new radio access network, usually referred to as LTE (Long Term Evolution).

Architecturally, the 3GPP Evolved Packet Core (EPC) network is similar to an IP wireless network running PMIPv6 or MIPv6, as it relies on the Packet Data Network Gateway (PGW) anchoring services to provide mobile nodes with mobility support (see Figure 5). There are client-based and network-based mobility solutions in 3GPP, which for simplicity will be analyzed together. We next describe how 3GPP mobility protocols and several other completed or ongoing extensions can be deployed to meet some of the DMM requirements [RFC7333].
The GPRS Tunneling Protocol (GTP) [SDO-3GPP.29.060] [SDO-3GPP.29.281] [SDO-3GPP.29.274] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces). In a similar way to PMIPv6, it can handle mobility without requiring the involvement of the mobile nodes. In this case, the mobile node functionality is provided in a proxy manner by the Serving Data Gateway (SGW), Evolved Packet Data Gateway (ePDG), or Trusted Wireless Access Gateway (TWAG [SDO-3GPP.23.402]).

3GPP specifications also include client-based mobility support, based on adopting the use of Dual-Stack Mobile IPv6 (DSMIPv6) [RFC5555] for the S2c interface [SDO-3GPP.24.303]. In this case, the User
Equipment (UE) implements the binding update functionality, while the home agent role is played by the PGW.

A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [SDO-3GPP.23.401] allows offloading some IP services at the local access network above the Radio Access Network (RAN) without the need to travel back to the PGW (see Figure 6).

Figure 6: LIPA scenario

SIPTO enables an operator to offload certain types of traffic at a network node close to the UE’s point of attachment to the access network, by selecting a set of GWs (SGW and PGW) that are geographically/topologically close to the UE’s point of attachment.

Figure 7: SIPTO architecture

LIPA, on the other hand, enables an IP addressable UE connected via a Home eNB (HeNB) to access other IP addressable entities in the same residential/enterprise IP network without traversing the mobile operator’s network core in the user plane. In order to achieve this, a Local GW (LGW) collocated with the HeNB is used. LIPA is established by the UE requesting a new Public Data Network (PDN) connection to an access point name for which LIPA is permitted, and
the network selecting the Local GW associated with the HeNB and enabling a direct user plane path between the Local GW and the HeNB.

```
+---------------+------  +----------+        +-------------+    =====
|Residential   |  | HeNB |  | Backhaul |  |Mobile       |   ( IP  )
|Enterprise    |..|------|..|          |..|Operator     |..(Network)
|Network       |  | LGW  |  |          |  |Core network |   ======
+---------------+------  +----------+        +-------------+
```

Figure 8: LIPA architecture

The 3GPP architecture specifications also provide mechanisms to allow discovery and selection of gateways [SDO-3GPP.29.303]. These mechanisms enable decisions taking into consideration topological location and gateway collocation aspects, relying upon the DNS as a "location database."

Both SIPTO and LIPA have a very limited mobility support, especially in 3GPP specifications up to Rel-12. Briefly, LIPA mobility support is limited to handovers between HeNBs that are managed by the same LGW (i.e., mobility within the local domain). There is no guarantee of IP session continuity for SIPTO.

5. Gap analysis

This section identifies the limitations in the current practices, described in Section 4, with respect to the DMM requirements listed in [RFC7333].

5.1. Distributed mobility management - REQ1

According to requirement REQ1 stated in [RFC7333], IP mobility, network access and forwarding solutions provided by DMM must make it possible for traffic to avoid traversing a single mobility anchor far from the optimal route.

From the analysis performed in Section 4, a DMM deployment can meet the requirement "REQ1 Distributed mobility management" usually relying on the following functions:

- Multiple (distributed) anchoring: ability to anchor different sessions of a single mobile node at different anchors. In order
to provide improved routing, some anchors might need to be placed closer to the mobile node or the corresponding node.

- Dynamic anchor assignment/re-location: ability to i) assign the initial anchor, and ii) dynamically change the initially assigned anchor and/or assign a new one (this may also require the transfer of mobility context between anchors). This can be achieved either by changing anchor for all ongoing sessions or by assigning new anchors just for new sessions.

**GAP1-1:** Both the main client- and network-based IP mobility protocols, namely (DS)MIPv6 and PMIPv6 allow deploying multiple anchors (i.e., home agents and localized mobility anchors), thereby providing the multiple anchoring function. However, existing solutions only provide an initial anchor assignment, thus the lack of dynamic anchor change/new anchor assignment is a gap. Neither the HA switch nor the LMA runtime assignment allows changing the anchor during an ongoing session. This actually comprises several gaps: ability to perform anchor assignment at any time (not only at the initial MN’s attachment), ability of the current anchor to initiate/trigger the relocation, and ability to transfer registration context between anchors.

**GAP1-2:** Dynamic anchor assignment may lead the MN to manage different mobility sessions served by different mobility anchors. This is not an issue with client based mobility management where the mobility client natively knows the anchor associated with each of its mobility sessions. However, there is one gap, as the MN should be capable of handling IP addresses in a DMM-friendly way, meaning that the MN can perform smart source address selection (i.e., deprecating IP addresses from previous mobility anchors, so they are not used for new sessions). Besides, managing different mobility sessions served by different mobility anchors may raise issues with network based mobility management. In this case, the mobile client located in the network, e.g., MAG, usually retrieves the MN’s anchor from the MN’s policy profile as described in Section 6.2 of [RFC5213]. Currently, the MN’s policy profile implicitly assumes a single serving anchor and thus does not maintain the association between home network prefix and anchor.

**GAP1-3:** The consequence of the distribution of the mobility anchors is that there might be more than one available anchor for a mobile node to use, which leads to an anchor discovery and selection issue. Currently, there is no efficient mechanism specified to allow the dynamic discovery of the presence of
nodes that can play the anchor role, discovering their capabilities and selecting the most suitable one. There is also no mechanism to allow selecting a node that is currently anchoring a given home address/prefix (capability sometimes required to meet REQ#2). However, there are some mechanisms that could help to discover anchors, such as the Dynamic Home Agent Address Discovery (DHAAD) [RFC6275], the use of the home agent flag (H) in Router Advertisements (which indicates that the router sending the Router Advertisement is also functioning as a Mobile IPv6 home agent on the link) or the MAP option in Router Advertisements defined by HMIPv6. Note that there are 3GPP mechanisms providing that functionality defined in [SDO-3GPP.29.303].

Regarding the ability to transfer registration context between anchors, there are already some solutions that could be reused or adapted to fill that gap, such as Fast Handovers for Mobile IPv6 [RFC5568] -- to enable traffic redirection from the old to the new anchor --, the Context Transfer protocol [RFC4067] -- to enable the required transfer of registration information between anchors --, or the Handover Keying architecture solutions [RFC6697], to speed up the re-authentication process after a change of anchor. Note that some extensions might be needed in the context of DMM, as these protocols were designed in the context of centralized client IP mobility, focusing on the access re-attachment and authentication.

GAP1-4: Also note that REQ1 is intended to prevent the data plane traffic from taking a suboptimal route. Distributed processing of the traffic may then be needed only in the data plane. Provision of this capability for distributed processing should not conflict with the use of a centralized control plane. Other control plane solutions such as charging, lawful interception, etc. should not be constrained by the DMM solution. On the other hand combining the control plane and data plane forwarding management (FM) function may limit the choice of solutions to those that distribute both data plane and control plane together. In order to enable distribution of only the data plane without distributing the control plane, it would be necessary to split the forwarding management function into the control plane (FM-CP) and data plane (FM-DP) components; there is currently a gap here.
5.2. Bypassable network-layer mobility support for each application session - REQ2

The requirement REQ2 for "bypassable network-layer mobility support for each application session" introduced in [RFC7333] requires flexibility in determining whether network-layer mobility support is needed. This requirement enables one to choose whether or not to use network-layer mobility support. The following two functions are also needed:

- Dynamically assign/relocate anchor: a mobility anchor is assigned only to sessions which use the network-layer mobility support. The MN may thus manage more than one session; some of them may be associated with anchored IP address(es), while the others may be associated with local IP address(es).

- Multiple IP address management: this function is related to the preceding and is about the ability of the mobile node to simultaneously use multiple IP addresses and select the best one (from an anchoring point of view) to use on a per-session/application/service basis. This requires MN to acquire information regarding the properties of the available IP addresses.

GAP2-1: The dynamic anchor assignment/relocation needs to ensure that IP address continuity is guaranteed for sessions that uses such mobility support (e.g., in some scenarios, the provision of mobility locally within a limited area might be enough from the mobile node or the application point of view) at the relocated anchor. Implicitly, when no applications are using the network-layer mobility support, DMM may release the needed resources. This may imply having the knowledge of which sessions at the mobile node are active and are using the mobility support. This is something typically known only by the MN, e.g., by its connection manager, and would also typically require some signaling support such as socket API extensions from applications to indicate to the IP stack whether mobility support is required or not. Therefore, (part of) this knowledge might need to be transferred to/shared with the network.

GAP2-2: Multiple IP address management provides the MN with the choice to pick the correct address, e.g., from those provided or not provided with mobility support, depending on the application requirements. When using client based mobility management, the mobile node is itself aware of the anchoring capabilities of its assigned IP addresses.
is not necessarily the case with network based IP mobility management; current mechanisms do not allow the MN to be aware of the properties of its IP addresses. For example, the MN does not know whether the allocated IP addresses are anchored. However, there are proposals, such as [I-D.bhandari-dhc-class-based-prefix], [I-D.korhonen-6man-prefix-properties] and [I-D.anipko-mif-mpvd-arch] that the network could indicate such IP address properties during assignment procedures. Although these individual efforts exist and they could be considered as attempts to fix the gap, there is no solution adopted as a work item within any IETF working group.

GAP2-3: The handling of mobility management to the granularity of an individual session of a user/device needs proper session identification in addition to user/device identification.

5.3. IPv6 deployment - REQ3

This requirement states that DMM solutions should primarily target IPv6 as the primary deployment environment. IPv4 support is not considered mandatory and solutions should not be tailored specifically to support IPv4.

All analyzed DMM practices support IPv6. Some of them, such as MIPv6/NEMO including the support of dynamic HA selection, MOBIKE, SIPTO also have IPv4 support. Some solutions, e.g., PMIPv6, also have some limited IPv4 support. In conclusion, this requirement is met by existing DMM practices.

5.4. Considering existing mobility protocols - REQ4

A DMM solution must first consider reusing and extending IETF-standardized protocols before specifying new protocols.

As stated in [RFC7333], a DMM solution could reuse existing IETF and standardized protocols before specifying new protocols. Besides, Section 4 of this document discusses various ways to flatten and distribute current mobility solutions. Actually, nothing prevents the distribution of mobility functions within IP mobility protocols. However, as discussed in Section 5.1 and Section 5.2, limitations exist.

The 3GPP data plane anchoring function, i.e., the PGW, can also be distributed, but with limitations; e.g., no anchoring relocation, no context transfer between anchors and centralized control plane. The 3GPP architecture is also going in the direction of flattening with SIPTO and LiPA, though they do not provide full mobility support.
For example, mobility support for SIPTO traffic can be rather limited, and offloaded traffic cannot access operator services. Thus, the operator must be very careful in selecting which traffic to offload.

5.5. Coexistence with deployed networks/hosts and operability across different networks - REQ5

According to [RFC7333], DMM implementations are required to co-exist with existing network deployments, end hosts and routers. Additionally, DMM solutions are expected to work across different networks, possibly operated as separate administrative domains, when the necessary mobility management signaling, forwarding, and network access are allowed by the trust relationship between them. All current mobility protocols can co-exist with existing network deployments and end hosts. There is no gap between existing mobility protocols and this requirement.

5.6. Operation and management considerations - REQ6

This requirement actually comprises several aspects, as summarized below.

- A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later.

- A DMM solution has to describe in what environment and how it can be scalably deployed and managed.

- A DMM solution has to support mechanisms to test if the DMM solution is working properly.

- A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.

- A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.

- A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.

- A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.
A DMM solution is expected to be able to monitor the usage of the DMM protocol.

DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

GAP6-1: Existing mobility management protocols have not thoroughly documented how, or whether, they support the above list of operation and management considerations. Each of the above needs to be considered from the beginning in a DMM solution.

GAP6-2: Management information base (MIB) objects are currently defined in [RFC4295] for MIPv6 and in [RFC6475] for PMIPv6. Standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules is lacking.

5.7. Security considerations - REQ7

As stated in [RFC7333], a DMM solution has to support any security protocols and mechanisms needed to secure the network and to make continuous security improvements. In addition, with security taken into consideration early in the design, a DMM solution cannot introduce new security risks, or privacy concerns, or amplify existing security risks, that cannot be mitigated by existing security protocols and mechanisms.

Any solutions that are intended to fill in gaps identified in this document need to meet this requirement. At present, it does not appear that using existing solutions to support DMM has introduced any new security issues. For example, Mobile IPv6 defines security features to protect binding updates both to home agents and correspondent nodes. It also defines mechanisms to protect the data packets transmission for Mobile IPv6 users. Proxy Mobile IPv6 and other variations of mobile IP also have similar security considerations.

5.8. Multicast - REQ8

It is stated in [RFC7333] that DMM solutions are expected to allow the development of multicast solutions to avoid network inefficiency in multicast traffic delivery.

Current IP mobility solutions address mainly the mobility problem for unicast traffic. Solutions relying on the use of an anchor point for tunneling multicast traffic down to the access router, or to the mobile node, introduce the so-called "tunnel convergence problem." This means that multiple instances of the same multicast traffic can
converge to the same node, diminishing the advantage of using multicast protocols.

[RFC6224] documents a baseline solution for the previous issue, and [RFC7028] a routing optimization solution. The baseline solution suggests deploying a Multicast Listener Discovery (MLD) proxy function at the MAG, and either a multicast router or another MLD proxy function at the LMA. The routing optimization solution describes an architecture where a dedicated multicast tree mobility anchor or a direct routing option can be used to avoid the tunnel convergence problem.

Besides the solutions highlighted before, there are no other mechanisms for mobility protocols to address the multicast tunnel convergence problem.

5.9. Summary

We next list the main gaps identified from the analysis performed above:

GAP1-1: Existing solutions only provide an optimal initial anchor assignment, a gap being the lack of dynamic anchor change/new anchor assignment. Neither the HA switch nor the LMA runtime assignment allows changing the anchor during an ongoing session. MOBIKE allows change of GW but its applicability has been scoped to a very narrow use case.

GAP1-2: The MN needs to be able to perform source address selection. Proper mechanism to inform the MN is lacking to provide the basis for the proper selection.

GAP1-3: Currently, there is no efficient mechanism specified by the IETF that allows the dynamic discovery of the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one. However, the following mechanisms could help discovering anchors:

- Dynamic Home Agent Address Discovery (DHAAD): the use of the home agent (H) flag in Router Advertisements (which indicates that the router sending the Router Advertisement is also functioning as a Mobile IPv6 home agent on the link) and the MAP option in Router Advertisements defined by HMIPv6.

GAP1-4: While existing network-based DMM practices may allow the deployment of multiple LMAs and dynamically select the best
one, this requires to still keep some centralization in the control plane, to access the policy database (as defined in RFC5213). Although [I-D.ietf-netext-pmip-cp-up-separation] allows a MAG to perform splitting of its control and user planes, there is a lack of solutions/extensions that support a clear control and data plane separation for IETF IP mobility protocols in a DMM context.

**GAP2-1:** The information of which sessions at the mobile node are active and are using the mobility support need to be transferred to or shared with the network. Such mechanism has not been defined.

**GAP2-2:** The mobile node needs to simultaneously use multiple IP addresses with different properties. There is a lack of mechanism to expose this information to the mobile node which can then update accordingly its source address selection mechanism.

**GAP2-3:** The handling of mobility management has not been to the granularity of an individual session of a user/device before. The combination of session identification and user/device identification may be lacking.

**GAP6-1:** Mobility management protocols have not thoroughly documented how, or whether, they support the following list of operation and management considerations:

* A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later.

* A DMM solution has to describe in what environment and how it can be scalably deployed and managed.

* A DMM solution has to support mechanisms to test if the DMM solution is working properly.

* A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.

* A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.
A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.

A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.

A DMM solution is expected to be able to monitor the usage of the DMM protocol.

DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

GAP6-2: Management information base (MIB) objects are currently defined in [RFC4295] for MIPv6 and in [RFC6475] for PMIPv6. Standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules is lacking.

6. Security Considerations

The deployment of DMM using existing IP mobility protocols raises similar security threats as those encountered in centralized mobility management systems. Without authentication, a malicious node could forge signaling messages and redirect traffic from its legitimate path. This would amount to a denial of service attack against the specific node or nodes for which the traffic is intended.

Distributed mobility anchoring, while keeping current security mechanisms, might require more security associations to be managed by the mobility management entities, potentially leading to scalability and performance issues. Moreover, distributed mobility anchoring makes mobility security problems more complex, since traffic redirection requests might come from previously unconsidered origins, thus leading to distributed points of attack. Consequently, the DMM security design needs to account for the distribution of security associations between additional mobility entities and fulfill the security requirement of [RFC7333].

7. Contributors

This document has benefited to valuable contributions from

Charles E. Perkins
Huawei Technologies
EMail: charliep@computer.org
who had produced a matrix to compare the different mobility protocols and extensions against a list of desired DMM properties. They were useful inputs in the early work of gap analysis. He had continued to give suggestions as well as extensive review comments to this documents.

8. References

8.1. Normative References


8.2. Informative References


[IEEE.802-16.2009]  
"IEEE Standard for Local and metropolitan area networks  
Part 16: Air Interface for Broadband Wireless Access  
Systems", IEEE Standard 802.16, 2009,  
<http://standards.ieee.org/getieee802/  
download/802.16-2009.pdf>.

[RFC3963]  
Devarapalli, V., Wakikawa, R., Petrescu, A., and P.  
Thubert, "Network Mobility (NEMO) Basic Support Protocol",  

[RFC4066]  
Liebsch, M., Singh, A., Chaskar, H., Funato, D., and E.  
Shim, "Candidate Access Router Discovery (CARD)", RFC  
4066, July 2005.

[RFC4067]  
Loughney, J., Nakhjiri, M., Perkins, C., and R. Koodli,  

[RFC4225]  
Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E.  
Nordmark, "Mobile IP Version 6 Route Optimization Security  

[RFC4295]  
Keeni, G., Koide, K., Nagami, K., and S. Gundavelli,  
"Mobile IPv6 Management Information Base", RFC 4295, April  
2006.

[RFC4555]  
Eronen, P., "IKEv2 Mobility and Multihoming Protocol  
(MOBIKE)", RFC 4555, June 2006.

[RFC4640]  
Patel, A. and G. Giaretta, "Problem Statement for  
bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September  
2006.

[RFC4889]  
Ng, C., Zhao, F., Watari, M., and P. Thubert, "Network  
Mobility Route Optimization Solution Space Analysis", RFC  
4889, July 2007.

[RFC4960]  
4960, September 2007.

[RFC5014]  
Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6  
Socket API for Source Address Selection", RFC 5014,  
September 2007.

[RFC5026]  
Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6  


[SDO-3GPP.24.303] 3GPP, "Mobility management based on Dual-Stack Mobile IPv6; Stage 3", 3GPP TS 24.303 10.0.0, June 2013.


[SDO-3GPP.29.274] 3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 10.11.0, June 2013.

[SDO-3GPP.29.303]
3GPP, "Domain Name System Procedures; Stage 3", 3GPP TS 29.303 10.4.0, September 2012.

Authors’ Addresses

Dapeng Liu (editor)
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
China
Email: liudapeng@chinamobile.com

Juan Carlos Zuniga (editor)
InterDigital Communications, LLC
1000 Sherbrooke Street West, 10th floor
Montreal, Quebec H3A 3G4
Canada
Email: JuanCarlos.Zuniga@InterDigital.com
URI: http://www.InterDigital.com/

Pierrick Seite
Orange
4, rue du Clos Courtel, BP 91226
Cesson-Sevigne 35512
France
Email: pierrick.seite@orange.com

H Anthony Chan
Huawei Technologies
5340 Legacy Dr. Building 3
Plano, TX 75024
USA
Email: h.a.chan@ieee.org
Abstract

This document defines the requirements for Distributed Mobility Management (DMM) at the network layer. The hierarchical structure in traditional wireless networks has led primarily to centrally deployed mobility anchors. As some wireless networks are evolving away from the hierarchical structure, it can be useful to have a distributed model for mobility management in which traffic does not need to traverse centrally deployed mobility anchors far from the optimal route. The motivation and the problems addressed by each requirement are also described.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
1. Introduction

In the past decade a fair number of network-layer mobility protocols have been standardized [RFC6275] [RFC5944] [RFC5380] [RFC6301] [RFC5213]. Although these protocols differ in terms of functions and associated message formats, they all employ a mobility anchor to allow a mobile node to remain reachable after it has moved to a different network. The anchor point, among other tasks, ensures connectivity by forwarding packets destined to, or sent from, the mobile node. It is a centrally deployed mobility anchor in the sense that the deployed architectures today have a small number of these anchors and the traffic of millions of mobile nodes in an operator network are typically managed by the same anchor. Such a mobility anchor may still have to reside in the subscriber’s provider network even when the subscriber is roaming to a visited network, in order that certain functions such as charging and billing can be performed more readily by the provider’s network. An example provider network is a Third Generation Partnership Project (3GPP) network.

Distributed mobility management (DMM) is an alternative to the above centralized deployment. The background behind the interests to study DMM are primarily in the following.

(1) Mobile users are, more than ever, consuming Internet content including that of local Content Delivery Networks (CDNs). Such traffic imposes new requirements on mobile core networks for data traffic delivery. To prevent exceeding the available core network capacity, service providers need to implement new strategies such as selective IPv4 traffic offload (e.g., [RFC6909], 3GPP work items Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) [TS.23.401]) through alternative access networks such as Wireless Local Area Network (WLAN) [Paper-Mobile.Data.Offloading]. In addition, a gateway selection mechanism takes the user proximity into account within the Evolved Packet Core (EPC) [TS.29303]. Yet these mechanisms were not pursued in the past owing to charging and billing considerations which require solutions beyond the mobility protocol. Consequently, assigning a gateway anchor node from a visited network when roaming to the visited network has only recently been done and is limited to voice services.

Both traffic offloading and CDN mechanisms could benefit from the development of mobile architectures with fewer hierarchical levels introduced into the data path by the mobility management system. This trend of "flattening" the mobile networks works best for direct communications among peers in the same geographical area. Distributed mobility management in the flattening mobile networks would anchor the traffic closer to
Today’s mobile networks present service providers with new challenges. Mobility patterns indicate that mobile nodes often remain attached to the same point of attachment for considerable periods of time [Paper-Locating.User]. Specific IP mobility management support is not required for applications that launch and complete their sessions while the mobile node is connected to the same point of attachment. However, currently, IP mobility support is designed for always-on operation, maintaining all parameters of the context for each mobile subscriber for as long as they are connected to the network. This can result in a waste of resources and unnecessary costs for the service provider. Infrequent node mobility coupled with application intelligence suggest that mobility support could be provided selectively such as in [I-D.bhandari-dhc-class-based-prefix] and [I-D.korhonen-6man-prefix-properties], thus reducing the amount of context maintained in the network.

DMM may distribute the mobility anchors in the data-plane in flattening the mobility network such that the mobility anchors are positioned closer to the user; ideally, mobility agents could be collocated with the first-hop router. Facilitated by the distribution of mobility anchors, it may be possible to selectively use or not use mobility protocol support depending on whether such support is needed or not. It can thus reduce the amount of state information that must be maintained in various mobility agents of the mobile network. It can then avoid the unnecessary establishment of mechanisms to forward traffic from an old to a new mobility anchor.

This document compares distributed mobility management with centralized mobility management in Section 3. The problems that can be addressed with DMM are summarized in Section 4. The mandatory requirements as well as the optional requirements for network-layer distributed mobility management are given in Section 5. Finally, security considerations are discussed in Section 6.

The problem statement and the use cases [I-D.yokota-dmm-scenario] can be found in [Paper-Distributed.Mobility.Review].

2. Conventions used in this document

2.1. Terminology

All the general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], in the Proxy mobile IPv6 specification
[RFC5213], and in Mobility Related Terminology [RFC3753]. These terms include the following: mobile node (MN), correspondent node (CN), and home agent (HA) as per [RFC6275]; local mobility anchor (LMA) and mobile access gateway (MAG) as per [RFC5213], and context as per [RFC3753].

In addition, this draft introduces the following terms.

Centrally deployed mobility anchors

refer to the mobility management deployments in which there are very few mobility anchors and the traffic of millions of mobile nodes in an operator network are managed by the same anchor.

Centralized mobility management

makes use of centrally deployed mobility anchors.

Distributed mobility management

is not centralized so that traffic does not need to traverse centrally deployed mobility anchors far from the optimal route.

Hierarchical mobile network

has a hierarchy of network elements arranged into multiple hierarchical levels which are introduced into the data path by the mobility management system.

Flattening mobile network

refers to the hierarchical mobile network which is going through the trend of reducing its number of hierarchical levels.

Flatter mobile network

has fewer hierarchical levels compared to a hierarchical mobile network.

Mobility context

is the collection of information required to provide mobility management support for a given mobile node.
3. Centralized versus distributed mobility management

Mobility management is needed because the IP address of a mobile node may change as the node moves. Mobility management functions may be implemented at different layers of the protocol stack. At the IP (network) layer, mobility management can be client-based or network-based.

An IP-layer mobility management protocol is typically based on the principle of distinguishing between a session identifier and a forwarding address and maintaining a mapping between the two. In Mobile IP, the new IP address of the mobile node after the node has moved is the forwarding address, whereas the original IP address before the mobile node moves serves as the session identifier. The location management (LM) information is kept by associating the forwarding address with the session identifier. Packets addressed to the session identifier will first route to the original network which re-directs them using the forwarding address to deliver to the session. Re-directing packets this way can result in long routes. An existing optimization routes directly using the forwarding address of the host, and such is a host-based solution.

The next two subsections explain centralized and distributed mobility management functions in the network.

3.1. Centralized mobility management

In centralized mobility management, the location information in terms of a mapping between the session identifier and the forwarding address is kept at a single mobility anchor, and packets destined to the session identifier are forwarded via this anchor. In other words, such mobility management systems are centralized in both the control plane and the data plane (mobile node IP traffic).

Many existing mobility management deployments make use of centralized mobility anchoring in a hierarchical network architecture, as shown in Figure 1. Examples are the home agent (HA) and local mobility anchor (LMA) serving as the anchors for the mobile node (MN) and Mobile Access Gateway (MAG) in Mobile IPv6 [RFC6275] and in Proxy Mobile IPv6 [RFC5213] respectively. Cellular networks such as the 3GPP General Packet Radio System (GPRS) networks and 3GPP Evolved Packet System (EPS) networks employ centralized mobility management too. In the 3GPP GPRS network, the Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN) and Radio Network Controller (RNC) constitute a hierarchy of anchors. In the 3GPP EPS network, the Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) constitute another hierarchy of anchors.
3.2. Distributed mobility management

Mobility management functions may also be distributed in the data plane to multiple networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a nearby function with appropriate forwarding management (FM) capability.

DMM is distributed in the data plane, whereas the control plane may either be centralized or distributed [I-D.yokota-dmm-scenario]. The former case implicitly assumes separation of data and control planes as described in [I-D.wakikawa-netext-pmip-cp-up-separation]. While mobility management can be distributed, it is not necessary for other functions such as subscription management, subscription database, and network access authentication to be similarly distributed.
A distributed mobility management scheme for a flattening mobile network consisting of access nodes is proposed in [Paper-Distributed.Dynamic.Mobility]. Its benefits over centralized mobility management have been shown through simulations [Paper-Distributed.Centralized.Mobility]. Moreover, the (re)use and extension of existing protocols in the design of both fully distributed mobility management [Paper-Migrating.Home.Agents] [Paper-Distributed.Mobility.SAE] and partially distributed mobility management [Paper-Distributed.Mobility.PMIP] [Paper-Distributed.Mobility.MIP] have been reported in the literature. Therefore, before designing new mobility management protocols for a future distributed architecture, it is recommended to first consider whether existing mobility management protocols can be extended.

4. Problem Statement

The problems that can be addressed with DMM are summarized in the following:

PS1: Non-optimal routes

Forwarding via a centralized anchor often results in non-optimal routes, thereby increasing the end-to-end delay. The problem is manifested, for example, when accessing a nearby server or servers of a Content Delivery Network (CDN), or when receiving locally available IP multicast or sending IP multicast packets. (Existing route optimization is only a host-based solution. On the other hand, localized routing with PMIPv6 [RFC6705] addresses only a part of the problem where both the MN and the correspondent node (CN) are attached to the same MAG, and it is not applicable when the CN does not behave like an MN.)

PS2: Divergence from other evolutionary trends in network architectures such as distribution of content delivery.

Mobile networks have generally been evolving towards a flatter and flatter network. Centralized mobility management, which is non-optimal with a flatter network architecture, does not support this evolution.

PS3: Lack of scalability of centralized tunnel management and mobility context maintenance

Setting up tunnels through a central anchor and maintaining mobility context for each MN usually requires more concentrated resources in a centralized design, thus reducing scalability.
Distributing the tunnel maintenance function and the mobility context maintenance function among different network entities with proper signaling protocol design can avoid increasing the concentrated resources with an increasing number of MNs.

PS4: Single point of failure and attack

Centralized anchoring designs may be more vulnerable to single points of failures and attacks than a distributed system. The impact of a successful attack on a system with centralized mobility management can be far greater as well.

PS5: Unnecessary mobility support to clients that do not need it

IP mobility support is usually provided to all MNs. Yet it is not always required, and not every parameter of mobility context is always used. For example, some applications or nodes do not need a stable IP address during a handover to maintain session continuity. Sometimes, the entire application session runs while the MN does not change the point of attachment. Besides, some sessions, e.g., SIP-based sessions, can handle mobility at the application layer and hence do not need IP mobility support; it is then unnecessary to provide IP mobility support for such sessions.

PS6: Mobility signaling overhead with peer-to-peer communication

Wasting resources when mobility signaling (e.g., maintenance of the tunnel, keep alive signaling, etc.) is not turned off for peer-to-peer communication.

PS7: Deployment with multiple mobility solutions

There are already many variants and extensions of MIP as well mobility solutions at other layers. Deployment of new mobility management solutions can be challenging, and debugging difficult, when they co-exist with solutions already deployed in the field.

PS8: Duplicate multicast traffic

IP multicast distribution over architectures using IP mobility solutions (e.g., [RFC6224]) may lead to convergence of duplicated multicast subscriptions towards the downstream tunnel entity (e.g., MAG in PMIPv6). Concretely, when multicast subscription for individual mobile nodes is coupled with mobility tunnels (e.g., PMIPv6 tunnel), duplicate multicast subscription(s) is prone to be received through
5. Requirements

After comparing distributed mobility management against centralized deployment in Section 3 and describing the problems in Section 4, this section identifies the following requirements:

REQ1: Distributed mobility management

IP mobility, network access and forwarding solutions provided by DMM MUST enable traffic to avoid traversing single mobility anchor far from the optimal route.

This requirement on distribution is in the data plane only. It does not impose constraints on whether the control plane should be distributed or centralized. However, if the control plane is centralized while the data plane is distributed, it is implicit that the control plane and data plane need to separate (Section 3.2).

Motivation: This requirement is motivated by current trends in network evolution: (a) it is cost- and resource-effective to cache contents, and the caching (e.g., CDN) servers are distributed so that each user in any location can be close to one of the servers; (b) the significantly larger number of mobile nodes and flows call for improved scalability; (c) single points of failure are avoided in a distributed system; (d) threats against centrally deployed anchors, e.g., home agent and local mobility anchor, are mitigated in a distributed system.

This requirement addresses the problems PS1, PS2, PS3, and PS4 described in Section 4.

REQ2: Bypassable network-layer mobility support for each application session

DMM solutions MUST enable network-layer mobility but it MUST be possible for any individual active application session (flow) to not use it. Mobility support is needed, for example, when a mobile host moves and an application cannot cope with a change in the IP address. Mobility support is also needed when a mobile router changes its IP address as it moves together with a host and, in the presence of ingress filtering, an application in the host is interrupted. However
mobility support at the network-layer is not always needed; a mobile node can often be stationary, and mobility support can also be provided at other layers. It is then not always necessary to maintain a stable IP address or prefix for an active application session.

Different active sessions can also differ in whether network-layer mobility support is needed. IP mobility, network access and forwarding solutions provided by DMM MUST then enable the possibility of independent handling for each application session of a user or mobile device.

The handling of mobility management to the granularity of an individual session of a user/device SHOULD need proper session identification in addition to user/device identification.

Motivation: The motivation of this requirement is to enable more efficient forwarding and more efficient use of network resources by selecting an IP address or prefix according to whether mobility support is needed and by not maintaining context at the mobility anchor when there is no such need.

This requirement addresses the problems PS5 and PS6 described in Section 4.

REQ3: IPv6 deployment

DMM solutions SHOULD target IPv6 as the primary deployment environment and SHOULD NOT be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used.

Motivation: This requirement conforms to the general orientation of IETF work. DMM deployment is foreseen in mid-to long-term horizon, when IPv6 is expected to be far more common than today.

This requirement avoids the unnecessarily complexity in solving the problems in Section 4 for IPv4, which will not be able to use some of the IPv6-specific features.

REQ4: Existing mobility protocols

A DMM solution MUST first consider reusing and extending IETF-standardized protocols before specifying new protocols.

Motivation: Reuse of existing IETF work is more efficient and less error-prone.
This requirement attempts to avoid the need of new protocols development and therefore their potential problems of being time-consuming and error-prone.

REQ5: Coexistence with deployed networks/hosts and operability across different networks

A DMM solution may require loose, tight or no integration into existing mobility protocols and host IP stack. Regardless of the integration level, DMM implementations MUST be able to coexist with existing network deployments, end hosts and routers that may or may not implement existing mobility protocols. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when the needed mobility management signaling, forwarding, and network access are allowed by the trust relationship between them.

Motivation: (a) to preserve backwards compatibility so that existing networks and hosts are not affected and continue to function as usual, and (b) enable inter-domain operation if desired.

This requirement addresses the problem PS7 described in Section 4.

REQ6: Operation and Management considerations.

A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later. Different management protocols are available. For example:

(a) SNMP [RFC1157] with definition of standardized management information base MIB objects for DMM, that allows monitoring traffic steering in a consistent manner across different devices,

(b) NETCONF [RFC6241] with definition of standardized YANG [RFC6020] modules for DMM to achieve a standardized configuration,

(c) syslog [RFC3164] which is a one-way protocol allowing a device to report significant events to a log analyzer in a network management system.
(d) IP Flow Information Export (IPFIX) Protocol, which serves as a means for transmitting traffic flow information over the network [RFC7011], with a formal description of IPFIX Information Elements [RFC7012].

It is not the goal of the requirements document to impose which management protocol(s) should be used. An inventory of the management protocols and data models is covered in RFC 6632.

The following lists the operation and management considerations required for a DMM solution; the list may not be exhaustive and may be expanded according to the needs of the solutions:

A DMM solution MUST describe in what environment and how it can be scalably deployed and managed.

A DMM solution MUST support mechanisms to test if the DMM solution is working properly. For example, when a DMM solution employs traffic indirection to support a mobility session, implementations MUST support mechanisms to test that the appropriate traffic indirection operations are in place, including the setup of traffic indirection and the subsequent teardown of the indirection to release the associated network resources when the mobility session has closed.

A DMM solution SHOULD expose the operational state of DMM to the administrators of the DMM entities. For example, when a DMM solution employs separation between session identifier and forwarding address, it should expose the association between them.

When flow mobility is supported by a DMM solution, the solution SHOULD support means to correlate the flow routing policies and the observed forwarding actions.

A DMM solution SHOULD support mechanisms to check the liveness of forwarding path. If the DMM solution sends periodic update refresh messages to configure the forwarding path, the refresh period SHOULD be configurable and a reasonable default configuration value proposed. Information collected can be logged or made available with protocols such as SNMP [RFC1157], NETCONF [RFC6241], IPFIX [RFC7011], or syslog [RFC3164].

A DMM solution MUST provide fault management and monitoring
mechanisms to manage situations where update of the mobility session or the data path fails. The system must also be able to handle situations where a mobility anchor with ongoing mobility sessions fails.

A DMM solution SHOULD be able to monitor usage of DMM protocol. When a DMM solution uses an existing protocol, the techniques already defined for that protocol SHOULD be used to monitor the DMM operation. When these techniques are inadequate, new techniques MUST be developed.

In particular, the DMM solution SHOULD

(a) be able to monitor the number of mobility sessions per user as well as their average duration.

(b) provide indication on DMM performance such as

1 the handover delay which includes the time necessary to re-establish the forwarding path when the point of attachment changes,

2 the protocol reactivity which is the time between handover events such as the attachment to a new access point and the completion of the mobility session update.

(c) provide means to measure the signaling cost of the DMM protocol.

(d) if tunneling is used for traffic redirection, monitor

1 the number of tunnels,

2 their transmission and reception information,

3 the used encapsulation method and overhead

4 the security used at a node level.

DMM solutions SHOULD support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which SHOULD be created for DMM when needed for such configuration. However, if a DMM solution creates extensions to MIPv6 or PMIPv6, the allowed addition of the definition of management information base (MIB) objects to MIPv6 MIB [RFC4295] or PMIPv6 MIB [RFC6475] needed for the control and monitoring of
the protocol extensions SHOULD be limited to read-only objects.

Motivation: A DMM solution that is designed from the beginning for operability and manageability can avoid difficulty or incompatibility to implement efficient operations and management solutions.

These requirements avoid DMM designs that make operations and management difficult or costly.

REQ7: Security considerations

A DMM solution MUST support any security protocols and mechanisms needed to secure the network and to make continuous security improvements. In addition, with security taken into consideration early in the design, a DMM solution MUST NOT introduce new security risks, or amplify existing security risks, that cannot be mitigated by existing security protocols and mechanisms.

Motivation: Various attacks such as impersonation, denial of service, man-in-the-middle attacks, and so on, may be launched in a DMM deployment. For instance, an illegitimate node may attempt to access a network providing DMM. Another example is that a malicious node can forge a number of signaling messages thus redirecting traffic from its legitimate path. Consequently, the specific node or nodes to which the traffic is redirected may be under a denial of service attack, whereas other nodes do not receive their traffic. Accordingly, security mechanisms/protocols providing access control, integrity, authentication, authorization, confidentiality, etc. should be used to protect the DMM entities as they are already used to protect against existing networks and existing mobility protocols defined in IETF. Yet if a candidate DMM solution is such that even the proper use of these existing security mechanisms/protocols are unable to provide sufficient security protection, that candidate DMM solution is causing uncontrollable security problems.

This requirement prevents a DMM solution from introducing uncontrollable problems of potentially insecure mobility management protocols which make deployment infeasible because platforms conforming to the protocols are at risk for data loss and numerous other dangers, including financial harm to the users.
REQ8: Multicast considerations

DMM SHOULD enable multicast solutions to be developed to avoid network inefficiency in multicast traffic delivery.

Motivation: Existing multicast deployment have been introduced after completing the design of the reference mobility protocol, often leading to network inefficiency and non-optimal forwarding for the multicast traffic. Instead DMM should consider multicast early so that the multicast solutions can better consider efficiency nature in the multicast traffic delivery (such as duplicate multicast subscriptions towards the downstream tunnel entities). The multicast solutions should then avoid restricting the management of all IP multicast traffic to a single host through a dedicated (tunnel) interface on multicast-capable access routers.

This requirement addresses the problems PS1 and PS8 described in Section 4.

6. Security Considerations

Please refer to the discussion under Security requirement in Section 5.

7. IANA Considerations

None

8. Contributors

This requirements document is a joint effort among numerous participants working in a team. Valuable comments and suggestions in various reviews from the following area directors and IESG members have also contributed to much improvements: Russ Housley, Catherine Meadows, Adrian Farrel, Barry Leiba, Alissa Cooper, Ted Lemon, Brian Haberman, Stephen Farrell, Joel Jaeggli, Alia Atlas, and Benoit Claise. In addition to the authors, each of the following has made very significant and important contributions to the working group draft in this work:

Charles E. Perkins
Huawei Technologies
Email: charliep@computer.org
9. References

9.1. Normative References


9.2.  Informative References

[I-D.bhandari-dhc-class-based-prefix]

[I-D.korhonen-6man-prefix-properties]

[I-D.wakikawa-netext-pmip-cp-up-separation]

[I-D.yokota-dmm-scenario]
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

[Paper-Distributed.Centralized.Mobility]
[Paper-Distributed.Dynamic.Mobility]

[Paper-Distributed.Mobility.MIP]

[Paper-Distributed.Mobility.PMIP]

[Paper-Distributed.Mobility.Review]

[Paper-Distributed.Mobility.SAE]

[Paper-Locating.User]


[Paper-Mobile.Data.Offloading]


[TS.29303] 3GPP, "Domain Name System Procedures; Stage 3", 3GPP TR 23.303 11.2.0, September 2012.

Authors’ Addresses

H Anthony Chan (editor)
Huawei Technologies
5340 Legacy Dr. Building 3, Plano, TX 75024, USA
Email: h.a.chan@ieee.org

Dapeng Liu
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District, Beijing 100053, China
Email: liudapeng@chinamobile.com

Abstract

[RFC5014] specifies extension to socket API to allow application to specify the preference among multiple source addresses. [I-D.draft-korhonen-6man-prfix-properties] and [I-D.draft-bhandari-dhc-class-based-prefix-04] propose to extend router advertisement to carry the prefix property and class information. The mobile node can learn the prefix property and class information from the router advertisement message. This document proposes an extension to [RFC5014] to enable the application to select the distributed mobility management related prefixes.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 09, 2014.
1. Proposed Extension of RFC 5014

[RFC5014] defines socket API extension used for IPv6 source address selection. Application can use this API to override the default source address selection mechanism for IPv6. Currently, [RFC5014] defines the following types of source address selection preference:

- IPV6_PREFER_SRC_HOME /* Prefer Home address as source */
- IPV6_PREFER_SRC_COA /* Prefer Care-of address as source */
- IPV6_PREFER_SRC_TMP /* Prefer Temporary address as source */
- IPV6_PREFER_SRC_PUBLIC /* Prefer Public address as source */
- IPV6_PREFER_SRC_CGA /* Prefer CGA address as source */
- IPV6_PREFER_SRC_NONCGA /* Prefer a non-CGA address as source */

This document proposes to extend the above definition to add two new flags:
IPV6_PREFER_SRC_LOCAL_HNP:
Prefer to use locally allocated home network prefix.

IPV6_PREFER_SRC_REMOTE_HNP:
Prefer to use the home network prefix that allocated by other access router instead of the one that the MN currently attach.

2. Usage Example

This section gives usage example for this API extension.

[I-D.draft-ietf-dmm-best-practices-gap-analysis-01] and [I-D.draft-seite-dmm-dma-06] discuss the distributed mobility management practice. It introduces dynamic anchoring concept: the mobile node can have multiple mobility anchor points and the mobile node select the locally allocated IP address for the newly started application for optimized routing. The mobile node can continue to use the IP address allocated by previous anchor point for the on going session. When the on going session terminate, the mobile node will release the previous anchor point allocated IP address.

In the dynamic anchoring scenario, for the newly started application, it should use the IP address allocated by the local mobility anchor. The application can use IPV6_PREFER_SRC_LOCAL_HNP flag to select the local allocated IP address. For the on going session, the application can use IPV6_PREFER_SRC_REMOTE_HNP flag to select the previous mobility anchor allocated home address to guarantee the session continuity.

3. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

4. Security Considerations

TBD

5. Acknowledgements

TBD

6. References
6.1. Normative References


6.2. Informative References


Authors’ Addresses

Dapeng Liu
China Mobile
32 Xuanwumen West Street
Beijing, Xicheng District 100053
China
Phone: +86-13911788933
Email: liudapeng@chinamobile.com

Hui Deng
China Mobile
32 Xuanwumen West Street
Beijing, Xicheng District 100053
China
Email: denghui@chinamobile.com
Abstract

This document discusses the SDN mobility problem and potential solutions.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 09, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Table of Contents

1. Introduction .................................................. 2
2. Conventions and Terminologies ............................... 2
   2.1. Conventions used in this document .................... 2
   2.2. Terminology ............................................ 2
3. Motivation of SDN mobility ................................. 2
4. SDN mobility problem analysis and potential solutions ...... 3
   4.1. Enhance SDN to support mobility tunnel handling ........ 3
   4.2. Routing based SDN mobility support ................... 4
5. Security Considerations ..................................... 5
6. IANA Considerations ......................................... 5
7. References .................................................. 5
   7.1. Normative References .................................. 5
   7.2. Informative References ................................. 5
Authors’ Addresses ............................................. 6

1. Introduction

Software defined networking provides a very flexible way to process IP packets and flows. It decouples the control and forwarding function of traditional IP appliance. IP mobility support has been specified by IETF. There is currently not much discussion regarding the mobility support in SDN network. This document discusses the motivation, problem and potential solution of the mobility support in SDN network.

2. Conventions and Terminologies

2.1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.2. Terminology

SDN: Software Defined Networking

3. Motivation of SDN mobility

IP mobility support has been specified in IETF for years. Both [RFC2002], [RFC3775], [RFC5555],[RFC5213] share the similar idea that it introduce an anchoring point to maintain the mapping of the home address and routing address of the mobile node. It uses tunnel to encapsulate the user traffic so that the application layer is not aware of the mobility event.
IP protocol has been used intensively in current cellular network architecture. For example, in LTE network architecture, IP support is enabled in the data plane. Also in the control plane and mobility support, IP mobility protocol is used. Both S2a/S2b/S2c interface is specified that can based on IP mobility protocol.

There is ongoing research work and discussions of using SDN in cellular network. SDN can provide the IP packets processing ability for the cellular core network. Mobility support is critical for the cellular core network. If mobility can be supported by SDN, the cellular core network can be significantly simplified. The data plane traffic routing can also be optimized. The following figure shows an architecture of the cellular core network that build upon SDN concept.

```
+--------------------+      +--------------+        +----------+
|mobility management |      | Charging     |        | Policy   |
+--------------------+      +--------------+        +----------+
                  +----------------------|----------------------|------------
                  |                            controller
                  +---------------------------------------------------------------------
                  +---------------------------------|-----------------------------------
                  |           forwarding and packet switching function
                  |                                    +---------------------------------------------------------------------
                  |                                    +---------------------------------|-----------------------------------
                  |                      wireless access network
                  +---------------------------------------------------------------------
                  +---------------------------------------------------------------------
```

Figure 1. SDN based Mobile core network

4. SDN mobility problem analysis and potential solutions

The purpose of mobility management is to maintain the session continuity from the application’s perspective. Normally, when a mobile node change its attachment point, its IP address will be changed accordingly. If there is no mobility support, the application layer session will be broken. For example, TCP session can not survive when the source IP address changes.

There are several potential ways for SDN network to support mobility. The following sections will discuss the potential solution in detail.

4.1. Enhance SDN to support mobility tunnel handling.

Current mobility protocol mainly follows the concept of mobility anchor. Mobility anchor point maintain the mapping of home address
and routing address. For example, in Mobile IP, the home agent maintain the mapping of home address and care of address. When the care of address changes due to mobile node’s movement, the foreign agent or the mobile node will send binding update request to the home agent to update the binding cache entry. The foreign agent or the mobile node will set up bi-directional tunnel towards the home agent. All the user traffic will be encapsulated in the bi-directional tunnel.

To enable SDN to support mobility, one potential solution is to enable the SDN controller and SDN forwarding function to support IP mobility protocol related tunnelling processing.

```
+-------------------+
|mobility management|
+-------------------+
                   API
                   +-----------------+
                   | controller |
                   +--------------+
                   |
                   +---------------+
                   | FA/MAG |
                   +-------+
                   | FA/MAG |
                   +-------+  LMA/HA
```

Figure 2. Enhance SDN to support mobility tunnel processing

The mobility management function could run on top of the controller. The controller controls the forwarding function. To support mobility, the mobility management function monitors the mobile node’s movement event. When the FA/MAG detects the mobile node’s movement, it needs to update the binding cache entry that maybe maintained in the mobility management function. The mobility management function then control the forwarding function(FA/MAG) to do the mobility tunnel processing. When the packets arrives at the LMA/HA, the mobility management function will control the forwarding function to decapsulate the packets and forward the packets to the Internet.

4.2. Routing based SDN mobility support
SDN provides a very flexible way of packet and flow processing. It is in nature can react quickly on the routing changes of the network. When the mobile node changes its point of attachment, the forwarding function will notify the mobility management function running on top of the controller, the controller then calculate the forwarding rules based on the destination IP address of the IP packet. The controller then push the forwarding rules to the forwarding function and the IP packet will be forwarded accordingly. When the user session terminated, the mobility management function will delete the forwarding rules. In this manner, the application layer session continuity will be guaranteed since the mobile node’s IP address is not changed during the movement.

There are lots of interesting problems need to be solved to make SDN support mobility. For example, the forwarding function needs to detect the movement event of the mobile node and notify the controller and mobility management function in a timely manner. A routing path needs to be set up from the MAG/FA to the Internet access point in a timely manner. To achieve this, new protocol and mechanism may need to be defined in IETF.

5. Security Considerations

TBD

6. IANA Considerations

None

7. References

7.1. Normative References


7.2. Informative References


Authors’ Addresses

Dapeng Liu
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District, Beijing 100053, China
Email: liudapeng@chinamobile.com

Hui Deng
China Mobile
32 Xuanwumen West Street
Beijing, Xicheng District  100053
China

Email: denghui@chinamobile.com
Abstract

Mobile IP protocols provide IP session continuity to Mobile Nodes at the expense of creating triangular routes via a centralized Home Agent. Increased latency and network resource use, introduction of a single point of failure and a network choke point are among the undesirable side effects of the current protocols. This document describes an alternative approach where the Mobile Node makes use of dynamically-assigned Home Agent that is located close to the Corresponding Node.
1. Introduction

In the context of Mobile IP [RFC5563][RFC6275][RFC5213][RFC5944] following two attributes are defined for the IP service provided to the mobile hosts:

IP session continuity: The ability to maintain an ongoing IP session by keeping the same local end-point IP address throughout the session despite moving among different IP networks. The IP address of the host may change between two independent IP sessions, but that does not jeopardize the IP session continuity. IP session continuity is essential for mobile hosts to maintain ongoing IP sessions without any interruption.

IP address reachability: The ability to maintain the same IP address for an extended period of time. The IP address shall stay the same across independent IP sessions, and even in the absence of any IP session. The IP address may be published in a long-term registry (e.g., DNS), and it shall be available for serving incoming connections. IP address reachability is essential for mobile hosts to use specific/published IP addresses.

Mobile IP is designed to provide both IP session continuity and IP address reachability to mobile hosts. The basic operation of Mobile IP involves the following: Network assigning a fixed IP address to
the Mobile Node (the Home Address, HoA) from a fixed node (the Home Agent, HA), the HA receiving location updates from the Mobile Node (MN), and the HA intercepting IP packets on behalf of the MN and tunneling them to the MN. That way the MN ensures it can keep receiving IP packets irrespective of its movement and location in the network.

One obvious side effect of this approach is the creation of sub-optimal routing paths between the MN and the other nodes it is communicating with (the Corresponding Nodes, CN). The routing path between the MN and a CN has to traverse the HA. Unless the HA is already located on the path between the MN and the CN, the path traversing the HA would create a so-called triangular route which is longer than the direct path between the two end-points. Longer path yields additional transmission latency and use of network resources [I-D.ietf-dmm-requirements].

Furthermore, forcing all MN traffic via the HA would also create a bottleneck in the network by overloading a single network element. The cost of building and operating such a network would increase, whereas the overall network reliability would decrease [I-D.ietf-dmm-requirements].

The objective of the solution described in this document is to provide IP session continuity to MNs without creating the aforementioned side effects.

The solution does not cover support for IP address reachability. This is considered to be acceptable, because only a very small set of applications really need IP address reachability. Those are the applications that are running as servers. Such applications cannot avoid using standard Mobile IP since they need to accept incoming connections at a specific/published IP address.

2. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Solution in a Nutshell

The negative side effects of Mobile IP can be remedied if the HA were positioned on the direct path between the MN and the CN. That way the IP packets would naturally flow thru the HA and not follow a triangular route. But, this is not possible when a single/fixed IP address is assigned to the MN and it is served by a single HA at a fixed location [RFC5563][RFC6275][RFC5213][RFC5944] while the MN is
communicating with CNs that are located in multiple different locations in the Internet.

The solution proposed in this document utilizes HAs located near CNs (Corresponding Home Agent, CHA) to dynamically allocate a HoA to the MN (Corresponding Home Address, CHoA). Such an address will be used throughout the IP session between the MN and the CN. Given the topological proximity of the CHA to the direct path between the MN and the CN, it is expected that this solution would not have the negative side effects of providing IP session continuity.

CHA may be co-located with the CN, or located in the same site as the CN, or located in an ISP serving that site. Not all CNs may be served by a CHA. In case there is no CHA serving the CN, the MN and the CN may communicate using the HoA via the HA. It is expected that CHAs would be deployed for dominant content sites on the Internet (e.g., YouTube, Facebook, Netflix, etc.)

The MN may be using multiple applications at the same time, and each application may be using a different CHA. For example, the MN may be configured to use CHoA1 for App1 with CN1 via CHA1, and use CHoA2 for App2 with CN2 via CHA2 at the same time.

Figure 1 depicts the high-level message flow for setting up data path between the MN and the CN using a CHA.

```
+------+
<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
+------+
```

Assume the MN is already configured with an IP address allocated from the access network it is attached to. Let this IP address be called IPxs.
Step 1:
Application on the MN attempts to initiate communication with the CN.

Step 2:
Network stack on the MN resolves the CN hostname to the IP address of CN. In parallel with that, the stack also tries to resolve the cha.CN_hostname in order to discover the CHA serving the CN, if there is any.

Step 3:
If a CHA is discovered at Step 2, then the network stack sends a Binding Update to the CHA. The HoA in the Binding Update is set to unspecified IP address (0.0.0.0/::) in order to request a dynamically-allocated CHoA from the CHA.

Step 4:
A tunnel is setup between the MN and the CHA as a result of Step 3. The tunnel end-points are IPxs and IP address of CHA (IPcha).

Step 5:
The socket used by the application is bound to the CHoA. The end-to-end communication between the App and the CN uses CHoA and IP address of CN (IPcn). Those IP packets are tunneled between the MN and the CHA.

Figure 2 depicts the high-level message flow for re-establishing the MN-CHA tunnel when the MN performs an IP handover.

```
+--------+   MN
|        |   +-----+-
|        |   |      |
App      Stack     CHA      CN
|        |   |      |
[1]      |   |      |
|        |   |      |
--------[2]--->
|        |   |      |
|        |   =========[3]====
|        |   |      |
|        |   <---------[4]========>

Figure 2. IP handover.
```
Step 1:

IP stack of MN configures a new IP address from the new access network (IPxs2).

Step 2:

MN sends a Binding Update to the CHA, binding CHoA to IPxs2.

Step 3:

A new tunnel is setup between the MN and the CHA (between the IPxs2 and IPcha).

Step 4:

The application and the CN continue their end-to-end communication using the new tunnel. The end point IP addresses stay the same (CHoA and IPcn), therefore the underlying routing change is transparent to the communication end-points.

Figure 3 depicts the high-level message flow for tearing down the MN-CHA tunnel when the application closes the connection.

```
Figure 2. Tear down.
```

Step 1:

The application attempts to close the session with the CN.

Step 2:

The network stack closes the connection with the CN (e.g., TCP FIN).
Step 3:

The MN sends a Binding Update to the CHA in order to de-register the binding between the IPxs and the CHoA. Dynamically-allocated CHoA and the tunnel between the MN and the CHA are released at this step.

4. Details

This section provides a more detailed description of the proposed solution. The solution utilizes the standard Mobile IP protocol signaling. Unless otherwise stated, the protocol details in [RFC6275][RFC5944] apply to the Mobile IP processing described in the following sections.

4.1. Setup

Figure 4 depicts the detailed message flow for setting up data path between the MN and the CN using a CHA.
Step 1:
Application attempts to resolve the IP address of the CN by issuing a Socket API call (e.g., gethostbyname, getaddrinfo).

Step 2a:
DNS client on the MN sends a DNS request to the DNS server in order to resolve the IP address of the CN.

Step 2b:
In parallel with Step 2a, DNS client on the MN should also send a DNS request to the DNS server in order to resolve the IP address of cha.CN_hostname.

Steps 3a and 3b:
DNS server returns the results.

Step 4:
At some point, the application attempts to send its first packet to the CN by issuing a Socket API call (e.g., connect, sendto).

Step 5:
If Step 3b has produced an IP address for the CHA (which indicates availability of a CHA for the CN), then the MN shall send a Binding Update to the CHA. The Binding Update shall include a HoA that is set to the unspecified IP address (0.0.0.0 for IPv4, :: for IPv6).

Steps 6 and 7:
The CHA may need to authenticate the incoming Binding Update in order to authorize it. This step may require AAA [RFC2865][RFC3588] between the CHA and a AAA server.

Step 8:
The CHA shall return a Binding Acknowledgement to the MN. This message should contain a dynamically-allocated HoA. This HoA is regarded as a CHoA.

Step 9:
The MN shall configure the received CHoA on its stack. The MN and the CHA shall also setup a tunnel between the care-of address in the
Binding Update (the IPxs) and IPcha. The MN shall setup a routing table entry to forward any IP packet whose source address is CHoA to the CHA via the tunnel. The CHA shall setup a routing table entry to forward any IP packet whose destination address is CHoA to the MN via the tunnel.

Step 10:

The MN shall assign the newly-configured CHoA as the source address for the socket used by the application. If a connection-oriented transport protocol is used, then a connection shall be established between (e.g., via TCP 3-way handshake) the CHoA and the IPcn (as obtained in Step 3a) via the tunnel between the MN and the CHA.

Step 11:

The communication between the application and the CN shall use CHoA and the IPcn as the end-points, and go via the tunnel between the MN and the CHA.

4.2. Handover

Figure 5 depicts the detailed message flow for re-establishing the MN-CHA tunnel when the MN performs an IP handover.

MN
------
|      |
|      |
|      |
|      |
| [1]  |
|      |
|======|

Figure 5. Detailed handover.

Step 1:

The MN configures a new IP address from the new access network (IPxs2).

Step 2:
When the IP address of the MN changes, the MN shall send a Binding Update to the CHA for informing the CHA about this change and binding the CHoA to the new IP address. The Binding Update shall include a CoA set to the IPxs2 and the HoA set to the CHoA.

Step 3:

The CHA shall process the incoming Binding Update according to [RFC6275][RFC5944] and return a Binding Acknowledgement.

Step 4:

The MN and the CHA shall setup a new tunnel with each other upon successful execution of Steps 3 and 4. The tunnel end-points shall be set to IPxs2 and IPcha. The CHA shall forward any incoming packet whose destination is CHoA towards the MN via the tunnel. The MN shall forward any outgoing packet whose source address is CHoA towards the CN via the tunnel.

4.3. Teardown

Figure 6 depicts the detailed message flow for tearing down the MN-CHA tunnel when the application closes the connection.

```
+------+
|      |
|      |
|      |
App  Stack               CHA     CN
|      |                  |       |
|      |-[1]->|                  |       |
|      |      |                  |       |
|      |      |<-=========[2]=------->|
|      |      |                  |       |
|      |
|      |-----------[3]--->|       |
|      |                  |       |
|      |<----------[4]----|       |
|      |                  |       |
```

Figure 6. Detailed tear down.

Step 1:

The application attempts to close the session with the CN.

Step 2:
The MN shall close the connection with the CN, if a connection-oriented transport is used (e.g., TCP, SCTP).

Step 3:

The MN shall send a Binding Update to CHA with lifetime set to 0.

Step 4:

The CHA shall send a Binding Acknowledgement back to the MN. The CHA and the MN shall release the tunnel, remove the forwarding entries for the CHoA. The CHA shall return the CHoA to the pool of available IP addresses. The MN shall unconfigure the CHoA on its stack.

If a connectionless protocol is used (e.g., UDP) between the MN and the CN, then the tear down may be triggered based on an inactivity timer or other indications.

5. Variation

A PMIP-based variation of this solution is under construction and will appear in a future version of this document.

6. Security Considerations

If the Binding Update message is not origin authenticated, then it may be leveraged for a DoS attack depleting the CHoA pool on the CHA.

This threat may be mitigated by allocating the CHoA from a very large address pool, such as 10.0.0.0/8 for IPv4, or a /64 prefix for IPv6. Depleting such a large address pool requires a significant brute-force attack. At that point the type of attack and its mitigations change and fall outside the scope of this document.

Another mitigation is to use origin authentication, replay and integrity protection on the Mobile IP messages [RFC6275][RFC5944][RFC4285] .

7. IANA Considerations

TBD

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@partner.samsung.com

Kisuk Kweon
Samsung
Suwon
South Korea

Email: kisuk.kweon@samsung.com
Jinsung Lee
Samsung
Suwon
South Korea

Email: js81.lee@samsung.com

Jungshin Park
Samsung
Suwon
South Korea

Email: shin02.park@samsung.com
Applications differ with respect to whether they need IP session continuity and/or IP address reachability. The network providing the same type of service to any mobile host and any application running on the host yields inefficiencies. This document describes a solution for taking the application needs into account in selectively providing IP session continuity and IP address reachability on a per-socket basis.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 04, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect
1. Introduction

In the context of Mobile IP [RFC5563][RFC6275][RFC5213][RFC5944], following two attributes are defined for the IP service provided to the mobile hosts:

IP session continuity: The ability to maintain an ongoing IP session by keeping the same local end-point IP address throughout the session despite moving among different IP networks. The IP address of the host may change between two independent IP sessions, but that does not jeopardize the IP session continuity. IP session continuity is essential for mobile hosts to maintain ongoing IP sessions without any interruption.

IP address reachability: The ability to maintain the same IP address for an extended period of time. The IP address shall stay the same across independent IP sessions, and even in the absence of any IP session. The IP address may be published in a long-term registry (e.g., DNS), and it shall be available for serving incoming (e.g., TCP) connections. IP address reachability is essential for mobile hosts to use specific/published IP addresses.

Mobile IP is designed to provide both IP session continuity and IP address reachability to mobile hosts. Architectures utilizing these protocols (e.g., 3GPP, 3GPP2, WIMAX) ensure that every one of the mobile hosts attached to the compliant networks enjoy these benefits. Every application running on each one of those mobile hosts is
subjected to the same treatment with respect to the IP session continuity and IP address reachability.

It should be noted that in reality not every application may need those benefits. IP address reachability is required for applications running as servers (e.g., a camera mounted on a bus). But, a typical client application (e.g., web browser) does not necessarily require IP address reachability. Similarly, IP session continuity is not required for all types of applications either. Applications performing brief communication (e.g., DNS client) can survive without having IP session continuity support.

Achieving IP session continuity and IP address reachability by using Mobile IP incur some cost. This solution forces the mobile host’s IP traffic to traverse a centrally-located router (Home Agent, HA), which incurs additional transmission latency and use of additional network resources, adds to the network CAPEX and OPEX, and decreases the reliability of the network with the introduction of a single point of failure [I-D.ietf-dmm-requirements]. Therefore, IP session continuity and IP address reachability should be used selectively.

Furthermore, even when an application needs IP session continuity, it may be able to satisfy that need by using a solution above the IP layer, such as MPTCP [RFC6824], SIP mobility [RFC3261], or an application-layer mobility solution. Those higher-layer solutions are not subject to the same issues that arise with the use of Mobile IP since they can utilize the most direct data path between the endpoints. But, if Mobile IP is being applied to the mobile host, those higher-layer protocols are rendered useless because their operation is inhibited by the Mobile IP. Since Mobile IP ensures the IP address of the mobile host remains fixed (despite the location and movement of the mobile host), the higher-layer protocols never detect the IP-layer movement and never engage in mobility management.

This document proposes a solution where the applications running on the mobile host can indicate whether they need IP session continuity or IP address reachability. The IP stack on the mobile host, in conjunction with the network, would provide the required type of IP service. It is for the benefit of both the users and the network operators not to engage an extra level of service unless it is absolutely necessary. So it is expected that applications and networks compliant with this specification would utilize this solution to use network resources more efficiently.

2. Notational Conventions
3. Solution

3.1. Types of IP Addresses

Three types of IP addresses are defined with respect to the mobility management.

- Home Network Anchored Address

This is what standard Mobile IP provides with a Home Address (HoA). The mobile host is configured a HoA from a centrally-located Home Network. Both IP session continuity and IP address reachability are provided to the mobile host with the help of a router in the Home Network (Home Agent, HA). This router acts as an anchor for the IP address of the mobile host.

- Access Network Anchored Address

This type of IP address provides IP session continuity but not IP address reachability. It is achieved by ensuring that the IP address used at the beginning of the session remains usable despite the movement of the mobile host. But the IP address may change after the end of ongoing IP sessions, therefore it does not exhibit persistence.

The IP address is allocated by a serving IP gateway. When the mobile host moves to another network, the previously serving gateway becomes an anchor gateway and starts treating the IP address as a Home Address with the help of the received binding updates. A tunnel is established between the anchor gateway and the current care-of address of the mobile host (whether configured on the host itself [RFC5944][RFC6275], or on the serving gateway [RFC5213][RFC5563]) for ensuring the session continuity using the same IP address.

- Unanchored Address

This type of IP address provides neither IP session continuity nor IP address reachability. The IP address is obtained from the serving IP gateway and it is not maintained across gateway changes. In other words, the IP address may be released and replaced by a new IP address when the IP gateway changes due to the mobile host’s mobility.
Applications running as servers at a published IP address require Home Network Anchored Address. Long-standing applications (e.g., an SSH session) may also require this type of address. They could use Access Network Anchored Address, but that can produce sub-optimal results if the mobile host ends up far from the anchor gateway. Enterprise applications that connect to an enterprise network via virtual LAN require Home Network Anchored Address.

Applications with short-lived transient IP sessions can use Access Network Anchored Address. For example: Email client, web browser, calendar, app store client, etc.

Applications with very short IP sessions, such as DNS client and instant messengers, can utilize Unanchored Address. Even though they could very well use Home or Access Network Anchored Addresses, the transmission latency would be the minimum when an Unanchored Address is used.

3.2. Granularity of Selection

The IP address type selection is made at per-socket granularity. Different parts of the same application may have different needs. For example, control part of the application may require Home Network Anchored Address in order to stay reachable, whereas data part of the application may be satisfied with Access Network Anchored Address.

3.3. On Demand Nature

At any point in time, a mobile host may have any mixture of IP addresses configured. Zero or more Unanchored, zero or more Access Network Anchored, and zero or more Home Network Anchored IP addresses may be available on the IP stack of the host. The mixture may be as a result of the host policy, or as a result of the application demand.

If an IP address of the requested type is not available, then the IP stack shall attempt to configure one. For example, a host may not always have a Home Network Anchored IP address available as this is rarely used. In case an application requests one, then the IP stack shall make an attempt to configure one using Mobile IP. If Mobile IP is not available to the host, or if its operation fails, then the IP stack shall fail the associated socket request. In case of successful Mobile IP operation, a Home Network Anchored IP Address gets configured on the mobile host. If another socket requests a Home Network Anchored IP address at a later time, then the same IP address may be served to that socket as well. When the last socket using the requested IP address is closed, the IP address may be released.
The following are matters of policy, which may be dictated by the host itself, the network operator, or the compliant network architecture:

- The initial set of IP addresses configured on the host at the boot time.
- Permission to grant various types of IP addresses to a requesting application.
- Determination of a default address type when an application does not make any explicit indication, whether it already supports the required API or it is a legacy application.

3.4. Conveying the Selection

The selection of the address type is conveyed from the applications to the IP stack in a way to influence the source address selection algorithm [RFC6724].

The current source address selection algorithm operates on the available set of IP addresses when selecting an address. According to the proposed solution, if the requested type IP address is not available at the time of the request, then the IP stack shall make an attempt to configure one such IP address. The selected IP address shall be compliant with the requested IP address type, whether it is selected among available addresses or dynamically configured. In the absence of a matching type (because it is not available and not configurable on demand), the source address selection algorithm shall return an empty set.

A Socket API-based interface for enabling applications to influence the source address selection algorithm is described in [RFC5014]. That specification defines IPV6_ADDR_PREFERENCES option at the IPPROTO_IPV6 level. That option can be used with setsockopt() and getsockopt() calls to set and get address selection preferences.

Furthermore, that RFC also specifies two flags that relate to IP mobility management: IPV6_PREFER_SRC_HOME and IPV6_PREFER_SRC_COA. These flags are used for influencing the source address selection to prefer either a Home Address or a Care-of Address.

Unfortunately, these flags do not satisfy the aforementioned needs due to the following reasons, therefore new flags are proposed in this document:

- Current flags indicate a "preference" whereas there is a need for indicating "requirement". Source address selection algorithm does
not have to produce an IP address compliant with the "preference", but it has to produce an IP address compliant with the "requirement".

- Current flags influence the selection made among available IP addresses. The new flags force the IP stack to configure a compliant IP address if none is available at the time of the request.

- The Home vs. Care-of Address distinction is not sufficient to capture the three different types of IP addresses described in Section 2.1.

The following new flags are defined in this document and they shall be used with Socket API in compliance with the [RFC5014]:

- IPV6_REQUIRE_HOME_ANCHORED /* Require Home Anchored address as source */
- IPV6_REQUIRE_ACCESS_ANCHORED /* Require Access Anchored address as source */
- IPV6_REQUIRE_UNANCHORED /* Require Unanchored address as source */

More than one of these flags may be set on the same socket. In that case, an IP address compliant with any one of them shall be selected.

When any of these new flags is used, then the IPV6_PREFER_SRC_HOME and IPV6_PREFER_SRC_COA flags, if used, shall be ignored.

These new flags are used with setsockopt()/getsockopt(), getaddrinfo(), and inet6_is_srcaddr() functions [RFC5014]. Similar with the setsockopt()/getsockopt() calls, getaddrinfo() call shall also trigger configuration of the required type IP address, if one is not already available. When the new flags are used with getaddrinfo() and the triggered configuration fails, the getaddrinfo() call shall ignore that failure (i.e., not return an error code to indicate that failure). Only the setsockopt() shall return an error when configuration of the requested type IP address fails.

Application of this solution to IPv4 is TBD.

4. Security Considerations

The setting of certain IP address type on a given socket may be restricted to privileged applications. For example, a Home Anchored IP Address may be provided as a premium service and only certain applications may be allowed to use them. Setting and enforcement of such privileges are outside the scope of this document.
5. IANA Considerations

TBD

6. References

6.1. Normative References


6.2. Informative References


Authors’ Addresses

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@partner.samsung.com

Kisuk Kweon
Samsung
Suwon
South Korea

Email: kisuk.kweon@samsung.com

Jinsung Lee
Samsung
Suwon
South Korea

Email: js81.lee@samsung.com

Jungshin Park
Samsung
Suwon
South Korea

Email: shin02.park@samsung.com